NORTH-HOLLAND
MATHEMATICAL LIBRARY

Elementary Theory of Numbers

W. SIERPINSKI
Editor: A. Schinzel

North-Holland
PWN – Polish Scientific Publishers

ELEMENTARY THEORY OF NUMBERS

North-Holland Mathematical Library

Board of Advisory Editors:

M. Artin, H. Bass, J. Eells, W. Feit, P.J. Freyd, F.W. Gehring, H. Halberstam, L.V. Hörmander, J.H.B. Kemperman, H.A. Lauwerier, W.A.J. Luxemburg, F.P. Peterson, I.M. Singer and A.C. Zaanen

VOLUME 31

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD

Elementary Theory of Numbers

W. SIERPIŃSKI

Editor: A. SCHINZEL
Mathematical Institute
of the Polish Academy of Sciences

1988
NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD

PWN–POLISH SCIENTIFIC PUBLISHERS
WARSZAWA

© PWN-POLISH SCIENTIFIC PUBLISHERS, 1988

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner.

Library of Congress Cataloging in Publication Data

Sierpiński, Wacław, 1882-1969.
Elementary theory of numbers.
(North-Holland mathematical library; vol. 31)
Based on the author's Teoria liczb.
1. Numbers, Theory of. I. Schinzel, Andrzej.
II. Sierpiński, Wacław, 1882-1969. Teoria liczb.
III. Title. IV. Series.
QA241.S477 1985 512'.72 86-16502
ISBN 0-444-86662-0

Second English edition revised and enlarged by A. Schinzel, published in 1988 in coedition between

ELSEVIER SCIENCE PUBLISHERS B.V.
P.O. Box 1991
1000 BZ Amsterdam
The Netherlands
and
PWN - POLISH SCIENTIFIC PUBLISHERS
Warszawa

First English edition: PWN-Polish Scientific Publishers, Warszawa 1964

Sole distributors for:

the U.S.A. and Canada
ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
52 Vanderbilt Avenue
New York, NY 10017
U.S.A.

Albania, Bulgaria, Cuba, Czechoslovakia, Democratic People's Republic of Korea, German Democratic Republic, Hungary, Mongolia, People's Republic of China, Poland, Romania, the USSR, Vietnam and Yugoslavia
ARS POLONA
Krakowskie Przedmieście 7
00-068 Warszawa

PRINTED IN POLAND

> *"The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge, its subject matter is tangible and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity."*
>
> *G.H. Hardy**

AUTHOR'S PREFACE

Contemporary mathematics comprises a number of branches whose traditional brief names, established for centuries, give no hint as to their actual scope and subject. This applies also to the Theory of Numbers, which, by the way, owing to its subject and methods, as well as its relation to other sciences, takes a special place among the various branches of mathematics.

The name of the Theory of Numbers might suggest that it is a kind of general theory concerning the notion of number and its generalizations which, starting from integers, introduces successively rational, real and complex numbers, and also some other kinds of numbers, and builds up a theory of operations on these numbers. This, however, is the subject of Higher Arithmetic. The subject of the Theory of Numbers is more special. It is concerned with the properties of integers, while the concept of integers and the theory of operations on them are taken ready-made from Higher Arithmetic and Algebra. However, the Theory of Numbers does not deal exclusively with integers. Many properties of integers have been discovered with the aid of irrational or complex numbers and many theorems about integers can be proved in a much simpler way if one makes use not only of irrational or complex numbers but also of the whole apparatus of the Calculus and the Theory of Functions. The part of the Theory of Numbers which makes extensive use of various parts of

---

* *Bull. Amer. Math. Soc.* 35 (1929), p. 818.

Analysis is called the Analytic Theory of Numbers, to be distinguished from the Elementary Theory of Numbers, which does not use the notion of limit.

The subject of this book is the Elementary Theory of Numbers, though a number of simple applications of the Analytic Theory of Numbers are also included. The book is prepared on the basis of two of my books issued between the years 1914 and 1959. These are

Teoria Liczb (Theory of Numbers), first edition, Warszawa 1914; second edition, Warszawa 1925; enlarged third edition, Warszawa-Wrocław 1950 (544 pages),

Teoria Liczb, Part II, Warszawa 1959 (487 pages).

To illustrate the progress which the Theory of Numbers has made in the last decade, it is sufficient to recall that the greatest prime number that was known in the year 1950 was $2^{127}-1$ of 39 digits and compare it with the number $2^{11213}-1$ of 8376 digits — the greatest prime number known to-day. In 1950 only 12 perfect numbers were known; to-day we know 23 of them.

In this book I have included various particular results of the Elementary Theory of Numbers that have been found in recent years in many countries.

I would like to express my thanks to Dr A. Hulanicki, who translated the manuscript of the book into English, to Doc. Dr A. Schinzel, who prepared the bibliography and added many valuable suggestions and footnotes concerning the results obtained recently, and to Dr A. Mąkowski, who helped me in reading the proofs. It is a pleasure to offer my thanks to Mrs. L. Izertowa, the editor of the book on behalf of PWN, who contributed so much to the preparation of the book so that it can be issued in the present form.

Wacław Sierpiński

Warsaw, May 1963

EDITOR'S PREFACE

As editor of the second edition of Sierpiński's "Elementary theory of numbers", I have respected his choice of the material and the order of its presentation. During the twenty years that elapsed since the publication of the first edition a considerable progress has been achieved in many of the questions treated there, thus I have construded my task as updating the relevant fragments of the book and modifying suitably the bibliography, eliminating also some minor errors. In this task I have been aided by my colleagues Jerzy Browkin and Andrzej Mąkowski to whom I express my sincere thanks. I acknowledge also with pleasure the hints for corrections received (sometimes indirectly) from Prof. John Brillhart, Prof. Eckford Cohen, Dr Waldemar Gorzkowski, Prof. Erich Michalup, Prof. M.V. Subbarao, Prof. Antoni Wakulicz and Prof. Gregory Wulczyn. Last but not least Mrs Krystyna Regulska from the office of the Polish Scientific Publishers has contributed to the publication of this book by taking care of all technical details, including the preparation of the new author index.

Andrzej Schinzel

Warsaw, February 1985

This page intentionally left blank

CONTENTS

Author's Preface v
Editor's Preface vii

CHAPTER I. DIVISIBILITY AND INDETERMINATE EQUATIONS OF FIRST DEGREE 1

1. Divisibility 1
2. Least common multiple 4
3. Greatest common divisor 5
4. Relatively prime numbers 6
5. Relation between the greatest common divisor and the least common multiple 8
6. Fundamental theorem of arithmetic 9
7. Proof of the formulae $(a_1, a_2, ..., a_{n+1}) = ((a_1, a_2, ..., a_n), a_{n+1})$ and $[a_1, a_2, ..., a_{n+1}] = [[a_1, a_2, ..., a_n], a_{n+1}]$ 13
8. Rules for calculating the greatest common divisor of two numbers 15
9. Representation of rationals as simple continued fractions 19
10. Linear form of the greatest common divisor 20
11. Indeterminate equations of m variables and degree 1 23
12. Chinese Remainder Theorem 28
13. Thue's Theorem 30
14. Square-free numbers 31

CHAPTER II. DIOPHANTINE ANALYSIS OF SECOND AND HIGHER DEGREES 32

1. Diophantine equations of arbitrary degree and one unknown 32
2. Problems concerning Diophantine equations of two or more unknowns 33
3. The equation $x^2+y^2 = z^2$ 35
4. Integral solutions of the equation $x^2+y^2 = z^2$ for which $x-y = \pm 1$ 42
5. Pythagorean triangles of the same area 46
6. On squares whose sum and difference are squares 50
7. The equation $x^4+y^4 = z^2$ 57
8. On three squares for which the sum of any two is a square 60
9. Congruent numbers 62
10. The equation $x^2+y^2+z^2 = t^2$ 66
11. The equation $xy = zt$ 69
12. The equation $x^4-x^2y^2+y^4 = z^2$ 73
13. The equation $x^4+9x^2y^2+27y^4 = z^2$ 75
14. The equation $x^3+y^3 = 2z^3$ 77
15. The equation $x^3+y^3 = az^3$ with $a > 2$ 82

16. Triangular numbers 84
17. The equation $x^2-Dy^2=1$ 88
18. The equations $x^2+k=y^3$ where k is an integer 101
19. On some exponential equations and others 109

CHAPTER III. PRIME NUMBERS 113

1. The primes. Factorization of a natural number m into primes 113
2. The Eratosthenes sieve. Tables of prime numbers 117
3. The differences between consecutive prime numbers 119
4. Goldbach's conjecture 123
5. Arithmetical progressions whose terms are prime numbers 126
6. Primes in a given arithmetical progression 128
7. Trinomial of Euler x^2+x+41 130
8. The Conjecture H 133
9. The function $\pi(x)$ 136
10. Proof of Bertrand's Postulate (Theorem of Tchebycheff) 137
11. Theorem of H. F. Scherk 148
12. Theorem of H.-E. Richert 151
13. A conjecture on prime numbers 153
14. Inequalities for the function $\pi(x)$ 157
15. The prime number theorem and its consequences 162

CHAPTER IV. NUMBER OF DIVISORS AND THEIR SUM 166

1. Number of divisors 166
2. Sums $d(1)+d(2)+\ldots+d(n)$ 169
3. Numbers $d(n)$ as coefficients of expansions 173
4. Sum of divisors 174
5. Perfect numbers 182
6. Amicable numbers 186
7. The sum $\sigma(1)+\sigma(2)+\ldots+\sigma(n)$ 188
8. The numbers $\sigma(n)$ as coefficients of various expansions 190
9. Sums of summands depending on the natural divisors of a natural number n 191
10. The Möbius function 192
11. The Liouville function $\lambda(n)$ 196

CHAPTER V. CONGRUENCES 198

1. Congruences and their simplest properties 198
2. Roots of congruences. Complete set of residues 203
3. Roots of polynomials and roots of congruences 206
4. Congruences of the first degree 209
5. Wilson's theorem and the simple theorem of Fermat 211
6. Numeri idonei 228
7. Pseudoprime and absolutely pseudoprime numbers 229

8. Lagrange's theorem 235
9. Congruences of the second degree 239

CHAPTER VI. EULER'S TOTIENT FUNCTION AND THE THEOREM OF EULER 245

1. Euler's totient function 245
2. Properties of Euler's totient function 257
3. The theorem of Euler 260
4. Numbers which belong to a given exponent with respect to a given modulus 263
5. Proof of the existence of infinitely many primes in the arithmetical progression $nk+1$ 268
6. Proof of the existence of the primitive root of a prime number 272
7. An nth power residue for a prime modulus p 276
8. Indices, their properties and applications 279

CHAPTER VII. REPRESENTATION OF NUMBERS BY DECIMALS IN A GIVEN SCALE 285

1. Representation of natural numbers by decimals in a given scale 285
2. Representations of numbers by decimals in negative scales 290
3. Infinite fractions in a given scale 291
4. Representations of rational numbers by decimals 295
5. Normal numbers and absolutely normal numbers 299
6. Decimals in the varying scale 300

CHAPTER VIII. CONTINUED FRACTIONS 304

1. Continued fractions and their convergents 304
2. Representation of irrational numbers by continued fractions 306
3. Law of the best approximation 312
4. Continued fractions of quadratic irrationals 313
5. Application of the continued fraction for $\sqrt{D}$ in solving the equations $x^2-Dy^2 = 1$ and $x^2-Dy^2 = -1$ 329
6. Continued fractions other than simple continued fractions 335

CHAPTER IX. LEGENDRE'S SYMBOL AND JACOBI'S SYMBOL 340

1. Legendre's symbol $\left(\frac{D}{p}\right)$ and its properties 340
2. The quadratic reciprocity law 346
3. Calculation of Legendre's symbol by its properties 351
4. Jacobi's symbol and its properties 352
5. Eisenstein's rule 355

CHAPTER X. MERSENNE NUMBERS AND FERMAT NUMBERS 360

1. Some properties of Mersenne numbers 360
2. Theorem of E. Lucas and D. H. Lehmer 363

3. How the greatest of the known prime numbers have been found 367
4. Prime divisors of Fermat numbers 369
5. A necessary and sufficient condition for a Fermat number to be a prime 375

CHAPTER XI. REPRESENTATIONS OF NATURAL NUMBERS AS SUMS OF NON-NEGATIVE kth POWERS 378

1. Sums of two squares 378
2. The average number of representations as sums of two squares 381
3. Sums of two squares of natural numbers 388
4. Sums of three squares 391
5. Representation by four squares 397
6. The sums of the squares of four natural numbers 402
7. Sums of $m \geqslant 5$ positive squares 408
8. The difference of two squares 410
9. Sums of two cubes 412
10. The equation $x^3+y^3 = z^3$ 415
11. Sums of three cubes 419
12. Sums of four cubes 422
13. Equal sums of different cubes 424
14. Sums of biquadrates 425
15. Waring's theorem 427

CHAPTER XII. SOME PROBLEMS OF THE ADDITIVE THEORY OF NUMBERS 431

1. Partitio numerorum 431
2. Representations as sums of n non-negative summands 433
3. Magic squares 434
4. Schur's theorem and its corollaries 439
5. Odd numbers which are not of the form 2^k+p, where p is a prime 445

CHAPTER XIII. COMPLEX INTEGERS 449

1. Complex integers and their norm. Associated integers 449
2. Euclidean algorithm and the greatest common divisor of complex integers 453
3. The least common multiple of complex integers 458
4. Complex primes 459
5. The factorization of complex integers into complex prime factors 463
6. The number of complex integers with a given norm 465
7. Jacobi's four-square theorem 469

Bibliography 482

Author index 505

Subject index 511

CHAPTER I

DIVISIBILITY AND INDETERMINATE EQUATIONS OF FIRST DEGREE

1. Divisibility

By *natural numbers* we mean the numbers 1, 2, ..., by *integers* we mean the natural numbers, the number zero and the negative numbers -1, -2, -3, ...

We say that an integer a is *divisible* by an integer b if there is an integer c such that $a = bc$. We then write

$$b \mid a.$$

We call b a *divisor* of a and a a *multiple* of b.

We write $b \nmid a$ if b does not divide a.

Since for each integer b we have $0 = 0 \cdot b$, every integer is a divisor of zero. Since for each integer a we have $a = a \cdot 1$, we see that 1 is a divisor of every integer.

Suppose now that x, y, z are integers such that

$$x \mid y \quad \text{and} \quad y \mid z. \tag{1}$$

Then there exist integers t and u such that $y = xt$ and $z = yu$. The number $v = tu$ is an integer (as the product of two integers). Thus, since $z = xv$, we obtain $x \mid z$. This proves that relations (1) imply the relation $x \mid z$ which means that a divisor of a divisor of an integer is a divisor of that integer. We express this by saying that the relation of divisibility of integers is *transitive*. It follows that if $x \mid y$, then $x \mid ky$ for every integer k.

It is easy to prove that a divisor of each of two given integers is a divisor of their sum and their difference. Moreover, if $d \mid a$ and $d \mid b$, then, for arbitrary integers x and y, $d \mid ax + by$.

In fact, the relations $d \mid a$ and $d \mid b$ imply that there exist integers k and l such that $a = kd$, $b = ld$, whence $ax + by = (kx + ly)d$ and consequently, since $kx + ly$ is an integer, $d \mid ax + by$.

Any two of the formulae $a = bc$, $-a = b(-c)$, $a = (-b)(-c)$, $-a = (-b)c$ are equivalent. Hence also any two of the formulae

$$b \mid a, \qquad b \mid -a, \qquad -b \mid a, \qquad -b \mid -a$$

are equivalent. Consequently while examining divisibility of integers we can restrict ourselves to the investigation of divisibility of natural numbers.

It follows from the definition of the relation $b \mid a$ that if $0 \mid a$, then $a = 0$. If, however, $a \neq 0$, then every divisor b of the integer a is different from zero and, consequently, $-b$ is also a divisor of a. Thus for an integer a, $a \neq 0$, the divisors b of a can be arranged in pairs $(b, -b)$. Therefore, in order to find all the divisors of an integer, it is sufficient to find the natural ones and then join to each of them the negative divisor of the same absolute value.

It seems at first sight that the notions of divisor and multiple are, in a sense, dual. It is much easier, however, to find the multiples of an integer than the divisors of it. In fact, the multiples of an integer a are, clearly, all the integers of the form ka, where k is an arbitrary integer. Consequently, the multiples of a form the sequence

$$\ldots, -2a, -a, 0, a, 2a, \ldots,$$

which is infinite in both directions. On the other hand, the task of finding the set of the divisors of a is by no means simple. This might seem strange, since the set of the divisors is finite and the set of the multiples is infinite.

If a natural number a is divisible by a natural number d, then $d \leqslant a$. Thus, in order to find all the positive divisors of an integer a, it suffices to divide a by the natural numbers $1, 2, \ldots, a$ successively and select those for which the quotient is an integer. Since for each natural number a the number of those quotients is finite, there exists a method, theoretically at least, for finding all the divisors of a given integer. The difficulty is, then, of a practical nature, and indeed for some natural numbers we are unable to find all the divisors. For instance, we cannot do this, for the time being at least, for the number $a = 2^{293}-1$, which has 89 digits. This turns out to be much too tedious a task even with the aid of computing machines. For the number 2^{293}, however, which is greater than a, we can, clearly, find all the natural divisors. They are 294 in number and form a geometric progression $1, 2, 2^2, 2^3, \ldots, 2^{293}$. We cannot find any of the non-trivial divisors of the number $2^{16384}+1$ either. We do not even know the exact number of them, which is, as we know greater than three (compare Chapter X).

Sometimes the divisors of a natural number have been found by the use of electronic computers. This was the case with the number $(18!-1):59 = 108514808571661$. With the aid of the computer SWAC.

D. H. Lehmer discovered that the number has exactly four natural divisors. They are 1, the number itself, 226663 and 478749547 (cf. Gabard [1], pp. 218-220). To the divisors of natural numbers and the number of them we shall return in Chapter IV.

The solution of the problem whether a given integer is divisible by another one may involve serious difficulties, which sometimes can be overcome by the use of electronic computers. For example, the fact that the number $a = 2^{65536}+1$ is divisible by the number $m = 825753601$ has been found in this way. The reason why this particular fact has been of special interest will be given later (Chapter X, § 4). The number a has 19729 digits, and so it would be a very tedious task even to write it down. However, the problem was not to divide a by m but to decide whether a is divisible by m or not, and the computations necessary for that could be simplified to the extent accessible to a computer.

We present here another example of the solution of a similar problem. This is the problem of divisibility of the number $2^{2^{23471}}+1$ by the number $5\cdot 2^{23473}+1$. The first number has more than 10^{7064} digits and it is clearly impossible to write down all of them; the second one has 7067 digits. Here again, owing to the special form of the first number, the necessary computations could be simplified to such an extent that electronic computers could be used. We return to this problem in Chapter X, § 4.

EXERCISES. 1. Prove that if a and b are natural numbers, then $a!\,b!\,|\,(a+b)!$.

PROOF. The theorem is true if at least one of the numbers a and b is equal to 1, since for each natural b we have $(b+1)! = b!(b+1)$, whence $1!\,b!\,|\,(1+b)!$. Thus the theorem is true for $a+b = 2$, since in this case $a = 1$ and $b = 1$. Suppose that n is a natural number greater than 2 and that the theorem is true for all natural numbers whose sum is equal to n. Let a and b be two natural numbers for which $a+b = n+1$. We already know that the theorem is true if at least one of the numbers a and b is equal to 1, and thus we may assume that $a > 1$ and $b > 1$. From the assumption that the theorem is true for the natural numbers whose sum is equal to n and from the equalities $(a-1)+b = n$, $a+(b-1) = n$ we infer that $(a-1)!\,b!\,|\,(a+b-1)!$ and $a!\,(b-1)!\,|\,(a+b-1)!$. But $(a+b)! = (a+b-1)!\,(a+b) = (a+b-1)!\,a+(a+b-1)!\,b$, and since $(a-1)!\,b!\,|\,(a+b-1)!$ and $(a-1)!\,a = a!$, $a!\,b!\,|\,(a+b-1)!\,a$. Similarly, by $a!\,(b-1)!\,|\,(a+b-1)!$, we deduce that $a!\,b!\,|\,(a+b-1)!\,b$. Hence, by the identity for $(a+b)!$, we conclude that $a!\,b!\,|\,(a+b)!$, which proves the theorem for natural numbers whose sum is equal to $n+1$. From this by induction the theorem follows for all natural a and b. □

2. Prove that, for a natural number k, the product $P = (a+1)(a+2)\dots(a+k)$ is divisible by $k!$.

PROOF. Plainly, $P = (a+k)!/a!$. Hence, in virtue of exercise 1 (for $b = k$), the theorem follows.

3. Prove that if $a_1, a_2, \dots, a_m$ are natural numbers ($m \geqslant 2$), then

$$a_1!\,a_2!\dots a_m! \mid (a_1+a_2+\dots+a_m)!$$

PROOF. As follows from exercise 1 the theorem is true for $m = 2$. Suppose it is true for a given natural number m and let $a_1, a_2, \dots, a_m, a_{m+1}$ be natural numbers. We then have

$$(a_1+a_2+\dots+a_m)!\,a_{m+1}! \mid (a_1+a_2+\dots+a_m+a_{m+1})!,$$

which, by the assumption that the theorem is true for the number m, implies the theorem for $m+1$. Thus by induction, the theorem follows.

In particular, for $m = 3$, $a_1 = n$, $a_2 = 2n$, $a_3 = 3n$, with $n = 1, 2, \dots$, we obtain

$$n!\,(2n)!\,(3n)! \mid (6n)!, \qquad n = 1, 2, \dots \quad \square$$

4. Prove that if S is a set of natural numbers such that for any two numbers of the set S their difference and their sum belong to S and d is the least natural number belonging to the set S, then S is the set of the natural multiples of the number d.

PROOF. By hypothesis, the sum of any two numbers belonging to the set S belongs to S. Hence, by an easy induction we infer that the sum of any finitely many numbers of the set S belongs to S. Accordingly, in the case of equal numbers, the numbers nd, with $n = 1, 2, \dots$ belong to S. In other words each natural multiple of the number d belongs to S.

On the other hand, suppose that k belongs to the set S and that k is not a multiple of d. Consequently, dividing k by d we obtain the positive reminder $r < d$. We have $k = qd+r$, where q is a natural number, for if $q = 0$, we would have $k \leqslant r < d$ and hence $k < d$, contrary to the assumption that d was the least number belonging to the set S. The number qd is then a natural multiple of the number d and as such belongs to the set S. Consequently, the natural number $r = k-qd$, as the difference of two numbers of the set S, belongs to S which is impossible, since $r < d$. This proves that each number of the set S is a natural multiple of the number d, and this completes the proof of the theorem. $\square$

2. Least common multiple

Let $a_1, a_2, \dots, a_n$ be a finite sequence of integers. Every integer which is divisible by each of the integers a_i ($i = 1, 2, \dots, n$) is called a *common multiple* of the integers $a_1, \dots, a_n$. Such is the product of the integers $a_1, a_2, \dots, a_n$, for instance. If at least one of the integers $a_1, a_2, \dots, a_n$ is zero, then clearly only the integer 0 is their common multiple. If, however, none of the integers a_i ($i = 1, 2, \dots, n$) is zero, there are infinitely many common multiples of these integers, e.g. all integers of the form $k\, a_1\, a_2 \dots a_n$, k being an integer. In this case there exist also common multiples which are natural numbers; for instance $|a_1\, a_2 \dots a_n|$, where $|x|$ denotes the modulus of the number x. In every set of natural numbers there exists the smallest number; consequently, the set of the common multiples of integers $a_1, a_2, \dots, a_n$, which are natural numbers, contains the smallest one; it is called the *least common multiple* of the integers $a_1, a_2 \dots, a_n$ and denoted by $[a_1, a_2, \dots, a_n]$.

THEOREM 1. *Every common multiple of natural numbers $a_1, a_2, \ldots, a_n$ is divisible by their least common multiple.*

PROOF. Suppose, contrary to Theorem 1, that there exists a common multiple M of the integers $a_1, a_2, \ldots, a_n$ which is not divisible by their least common multiple N. Let

$$M = qN + r,$$

where r is a natural number $< N$. Hence $r = M - qN$. Let i be any of the numbers $1, 2, \ldots, n$. Since M and N are multiples of the integer a_i, there exist integers x_i and y_i such that $M = x_i a_i$ and $N = y_i a_i$. Therefore $r = M - qN = (x_i - qy_i) a_i$, whence $a_i \mid r$ for all $i = 1, 2, \ldots, n$, which implies that the natural number r is a common multiple of the integers $a_1, a_2, \ldots, a_n$ and is smaller than their least common multiple N; this is clearly impossible. □

3. Greatest common divisor

Let S be a given (finite or infinite) set of integers such that at least one of them, for instance a_0, is different from zero. Every integer d which is a divisor of each of the integers of the set S is called a *common divisor* of the integers of the set S. Clearly, the integer 1 is an example of a common divisor of the integers of S.

Every integer d which is a common divisor of the integers of the set S is, clearly, a divisor of the natural number $|a_0|$, and so its modulus is less than $|a_0|$. It follows that the number of common divisors of the integers of the set S is finite, and therefore there exists the greatest one among them; that number is called the *greatest common divisor* of the integers of the set S, and is denoted by d_S. d_S is plainly a natural number. Now, let d denote an arbitrary common divisor of the integers of the set S and let $N = [d, d_S]$. Further, let a be an integer of the set S. We have $d \mid a$ and $d_S \mid a$, which proves that a is a common multiple of the divisors d and d_S, whence, by Theorem 1, $[d, d_S] \mid a$. The number $N = [d, d_S]$ is then a divisor of the integers of the set S and, since d_S is the greatest common divisor of those integers, $N \leqslant d_S$. But the natural number N, as the least common multiple of the numbers d and d_S, is divisible by d_S, whence $N \geqslant d_S$. Thus $N = d_S$, and so $d \mid d_S$. This proves the following

THEOREM 2. *If S is a set (finite or infinite) of integers among which at least one is different from zero, then there exists the greatest common divisor of* *the integers of the set S. Moreover, the greatest common divisor is divisible by any other common divisor of the integers of the set S.*

It can be proved (cf. Hensel [1]) that if $f(x)$ is a polynomial of degree n with integer coefficients and k is an arbitrary integer, then the greatest common divisor of the numbers $f(x)$, x running over the set of integers, is equal to the greatest common divisor of the following $n+1$ integers: $f(k)$, $f(k+1), f(k+2), \ldots, f(k+n)$. Thus, for instance, if $f(x) = x^3 - x$, then, in virtue of what we have stated above, the greatest common divisor of the integers $f(x)$, x being an integer, is equal to the greatest common divisor of the integers $f(-1) = 0, f(0) = 0, f(1) = 0, f(2) = 6$, i.e. it is equal to 6.

4. Relatively prime numbers

Two integers a and b whose greatest common divisor is equal to 1 are called *relatively prime.*

THEOREM 3. *Dividing each of two integers a and b by their greatest common divisor we obtain relatively prime numbers.*

PROOF. Let a and b be two integers, d their greatest common divisor and $a_1 = a/d$, $b_1 = b/d$. If the integers a_1 and b_1 were not relatively prime, their greatest common divisor d_1 would be greater than 1, and then we should have $a_2 = a_1/d_1$ and $b_2 = b_1/d_1$, a_2 and b_2 being integers. But then we would obtain the equalities $a = dd_1 a_2$, $b = dd_1 b_2$, implying that the integer dd_1 is a common divisor of the integers a and b, whence $dd_1 \leqslant d$, which is impossible, since $d_1 > 1$. This shows that the integers a_1 and b_1 must be relatively prime, which completes the proof of Theorem 3. □

The greatest common divisor of integers $a_1, a_2, \ldots, a_n$ is denoted by $(a_1, a_2, \ldots, a_n)$.

The argument used to prove Theorem 3 will also prove the following

THEOREM 3^a. *Dividing each of the integers $a_1, a_2, \ldots, a_n$ by their greatest common divisor we obtain integers whose greatest common divisor is equal to* 1.

Let r be a rational number (i.e. the ratio a/b of two integers a and b with $b \neq 0$). Multiplying, if necessary, the denominator of r by -1, we may assume that $b > 0$. If $(a, b) = d$, then putting $a/d = a_1$, $b/d = b_1$ we obtain, by Theorem 3, relatively prime numbers a_1 and b_1 with $b_1 > 0$, since b has been assumed to be > 0. We then have $r = a/b = a_1/b_1$. Thus every rational number can be written as a fraction whose numerator is an integer and denominator a natural number, the numerator and the denominator being relatively prime.

Now we prove that *if* $(a, b) = 1$ *and* $c \mid a$, *then* $(c, b) = 1$.

In fact, if $(c, b) = d$, then $d \mid b$ and $d \mid c$, whence, in virtue of $c \mid a$, we obtain $d \mid a$. Consequently, d is a common divisor of the integers a and b, thus, by Theorem 2, it is a divisor of their greatest common divisor $= 1$, whence $d = 1$, which proves that $(c, b) = 1$.

For every finite sequence of natural numbers $a_1, a_2, \ldots, a_n$ we can easily find a natural number a which is relatively prime to every number of the sequence. Such is, for instance, the number $a = a_1 a_2 \ldots a_n + 1$; for, every common divisor d_i of the integers a and a_i, where i is any number of the numbers $1, 2, \ldots, n$, is also a divisor of the number $a_1 a_2 \ldots a_n$ and hence a divisor of the difference $a - a_1 a_2 \ldots a_n = 1$, so it is equal to 1.

From this we can easily conclude that there exists an infinite sequence of natural numbers such that any two different elements of it are relatively prime. But the formula obtained in this way for the nth term of this sequence would not be simple. A much simpler example of a sequence F_k whose any two different terms are relatively prime is obtained by setting $F_k = 2^{2^k} + 1$ $(k = 0, 1, 2, \ldots)$. In fact, let m and n be two integers, with $m > n \geqslant 0$. As is well known for each integer x and natural number k we have $x - 1 \mid x^k - 1$ (since $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \ldots + x + 1)$). Applying this to $x = 2^{2^{n+1}}$, $k = 2^{m-n-1}$ we obtain that $2^{2^{n+1}} - 1 \mid 2^{2^m} - 1$. Since $F_n = 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1$ and $2^{2^m} - 1 = F_m - 2$, we have $F_n \mid F_m - 2$. Hence if $d \mid F_n$ and $d \mid F_m$, then $d \mid F_m - 2$, which implies $d \mid 2$. But d, as a divisor of an odd number F_m, is an odd number, and thus the relation $d \mid 2$ implies $d \mid 1$, which proves that $(F_m, F_n) = 1$ for $m > n \geqslant 0$, as required.

It is worth-while noting that the following generalization of the above is also true. If a and b are two relatively prime integers and if $2 \mid ab$, then any two different numbers in the sequence $a^{2^k} + b^{2^k}$ $(k = 0, 1, 2, \ldots)$ are relatively prime.

One can prove that if k is a natural number $\leqslant 16$, then among every k consecutive natural numbers there exists at least one number relatively prime to each of the remaining $k-1$ numbers (Pillai [4]). On the other hand, one can prove that for each natural number $k \geqslant 17$ there exists a sequence of k consecutive natural numbers $m, m+1, \ldots, m+k-1$ such that none of the numbers of the sequence is relatively prime to each of the others (cf. Pillai [5], [6] and Brauer [2]). Here we prove this statement for $k = 17$. We claim that in this case the number $m = 2184$ satisfies our conditions. In other words, we assert that none of the consecutive natural numbers 2184, 2185, ..., 2200 is relatively prime to each of the other numbers of the sequence.

None of the numbers of the sequence which is divisible by anyone of the numbers, 2, 3, 5, 7, is relatively prime to each of the other numbers of the sequence, since for each $n = 2, 3, 5, 7$ there are at least two numbers in the sequence divisible by n. There are only two other numbers in the sequence, 2189 and 2197, but the first of them as well as the number 2200, is divisible by 11 and the second one, as well as the number 2184, is divisible by 13.

EXERCISES. **1.** Prove that if m and n are natural numbers and m is odd, then $(2^m-1, 2^n+1) = 1$.

PROOF (J. Browkin). Let d be the greatest common divisor of the numbers 2^m-1 and 2^n+1. d is an odd number and $2^m-1 = kd$, $2^n+1 = ld$, where k and l are natural numbers. Hence $2^m = kd+1$, $2^n = ld-1$, whence $2^{mn} = (kd+1)^n = td+1$, $2^{mn} = (ld-1)^m = ud-1$, where t and u are natural numbers.

Consequently, since $td+1 = ud-1$, we have $d \mid 2$, and this in view of d being odd, implies that $d = 1$. ☐

2. Prove that for each natural number n we have $(n!+1, (n+1)!+1) = 1$.

PROOF. If $d \mid n!+1$ and $d \mid (n+1)!+1$, then using the equality $(n!+1)(n+1) = (n+1)!+n+1$, we see that $d \mid (n+1)!+n+1$, whence $d \mid n$ and, since $d \mid n!+1$, we have $d \mid 1$. ☐

5. Relation between the greatest common divisor and the least common multiple

THEOREM 4. *The product of two natural numbers is equal to the product of their least common multiple and their greatest common divisor.*

PROOF. Let a and b be two natural numbers, and let $N = [a, b]$. Since ab is clearly a common multiple of the numbers a and b, Theorem 1 implies that $N \mid ab$. Let $ab = dN$, where d is a natural number. Since N is a common multiple of a and b, we have $N = ka = lb$, where k and l are natural numbers. From this we obtain $ab = dN = dka = dlb$, and hence $a = dl$ and $b = dk$, which proves that d is a common divisor of the numbers a and b.

Now, let t denote an arbitrary common divisor of the numbers, a and b. We have $a = ta_1$, $b = tb_1$, which implies that the number $ta_1 b_1$ is a common multiple of the numbers a and b. Therefore, by Theorem 1, we have $N \mid ta_1 b_1$. Hence, for an integer u, we obtain $ta_1 b_1 = Nu$. But $dN = ab = t^2 a_1 b_1$, whence $tNu = dN$. Consequently, $d = tu$ and $t \mid d$. Thus the natural number d is a common divisor of the numbers a and b and, moreover, every common divisor of these numbers divides d; this proves that d is the greatest common divisor of the numbers a and b, which, in view of the formula $ab = dN$, completes the proof of Theorem 4. ☐

An important special case of Theorem 4 is obtained when the natural numbers a and b are relatively prime, i.e. when $d = (a, b) = 1$. Then the formula $ab = Nd$ implies $N = ab$. This proves the following

COROLLARY. *The least common multiple of two relatively prime natural numbers is equal to their product.*

6. Fundamental theorem of arithmetic

Let a and b be two relatively prime natural numbers and c a natural number such that $b \mid ac$. The number ac is divisible by each of the numbers a and b, therefore, by Theorem, 1, it is also divisible by their least common multiple, which, in virtue of the corollary to Theorem 4, is equal to ab. Thus $ac = tab$, where t is an integer, whence $c = tb$, and therefore $b \mid c$. Thus we have proved the following

THEOREM 5. *A natural number which divides the product of two natural numbers and is relatively prime to one of them is a divisor of the other.*

Theorem 5 is sometimes called the *fundamental theorem of arithmetic.* We have proved it for natural numbers, but, clearly, it remains true for all integers since the change of the sign does not affect divisibility of the numbers.

COROLLARY. *If a, b, c are integers such that $a \mid c$, $b \mid c$ and $(a, b) = 1$, then $ab \mid c$.*

PROOF. If $a \mid c$, then $c = at$, where t is an integer. Since $b \mid c$, we have $b \mid at$ and hence using both the assumption that $(a, b) = 1$ and Theorem 5 we obtain $b \mid t$, i.e. $t = bu$, where u is an integer; hence $c = at = abu$, and thus $ab \mid c$, as required. ☐

As an easy corollary to Theorem 5 we prove

THEOREM 6. *If* a, b, c *are integers such that* $(a, b) = (a, c) = 1$, *then* $(a, bc) = 1$.

PROOF. Let $d = (a, bc)$ and $d_1 = (b, d)$. We then have $d_1 \mid b$ and $d_1 \mid d$. Since $d \mid a$, $d_1 \mid a$; we see, in virtue of the fact that $d_1 \mid a$, $d_1 \mid b$ and $(a, b) = 1$ hold, that $d_1 = 1$. Thus $(b, d) = 1$. But, since $d = (a, bc)$, $d \mid bc$, which by Theorem 5 implies that $d \mid c$. In view of $d \mid a$ and by $(a, c) = 1$ we conclude that $d = 1$, i.e. $(a, bc) = 1$, as required. ☐

From this, by an easy induction, we derive

THEOREM 6^a. *Let* n *be a natural number* $\geqslant 2$. *If* $a_1, a_2, \ldots, a_n$ *and* a *are integers such that* $(a_i, a) = 1$ *holds for every* $i = 1, 2, \ldots, n$, *then* $(a_1 a_2 \ldots a_n, a) = 1$.

In other words, Theorem 6^a states that an integer, which is relatively prime to each of the given integers is relatively prime to their product.

Returning to Theorem 5 we see that the argument used for its proof will also prove the following generalization of it.

If a, b *and* c *are integers such that* $b \mid ac$, *then* $b \mid (a, b)(b, c)$.

Theorem 6^a has the following

COROLLARY 1. *If* $(a, b) = 1$ *and* n *is a natural number, then* $(a^n, b^n) = 1$.

PROOF. If $(a, b) = 1$, then, by Theorem 6^a (for $a_1 = a_2 = \ldots = a_n = a$), we have $(a^n, b) = 1$, whence, again by Theorem 6^a (for $a_1 = a_2 = \ldots = a_n = b$), we conclude that $(a^n, b^n) = 1$.

From Corollary 1 we derive

COROLLARY 2. *For natural numbers* a, b, n, *the relation* $a^n \mid b^n$ *implies the relation* $a \mid b$.

PROOF. Let $(a, b) = d$. We then have $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$. Hence, in view of Corollary 1, $(a_1^n, b_1^n) = 1$. Since $a^n \mid b^n$, or equivalently

$a_1^n d^n \mid b_1^n d^n$, we have $a_1^n \mid b_1^n$ and $a_1^n \mid (a_1^n, b_1^n)$, which proves that $a_1^n \mid 1$, whence $a_1 = 1$, $a = d$, and consequently, by $b = db_1 = ab_1$, $a \mid b$, as required. □

We note that for two natural numbers a and b the relation $a^a \mid b^b$ does not necessarily imply $a \mid b$. For instance it is easy to check that $4^4 \mid 10^{10}$, but $4 \nmid 10$; similarly $9^9 \mid 21^{21}$, but $9 \nmid 21$.

REMARK. The notion of divisibility of one number by another can be extended to real numbers in the following manner. Given two real numbers α and β we say that α divides β and write $\alpha \mid \beta$ if there exists an integer k such that $\beta = k\alpha$. In the case of this extended notion of divisibility, however, the relation $\alpha^2 \mid \beta^2$ does not necessarily imply the relation $\alpha \mid \beta$. For instance, $2 \mid 6$, but it is not true that $\sqrt{2} \mid \sqrt{6}$, since if it were, the latter relation would imply the existence of an integer k such that $\sqrt{6} = k\sqrt{2}$, which would give $k = \sqrt{3}$, whence $3 = k^2$ and thus $k > 1$, i.e. $k \geqslant 2$, and then $3 = k^2 \geqslant 4$, which, clearly, is untrue.

COROLLARY 3. *For natural numbers a, b and $n > 1$, the relation $a^n \mid 2b^n$ implies $a \mid b$.*

PROOF. Let $(a, b) = d$. Consequently, $a = da_1, b = db_1$, where $(a_1, b_1) = 1$. Hence, by Corollary 1, $(a_1^n, b_1^n) = 1$ and, in virtue of the relation $a^n \mid 2b^n$, we have $d^n a_1^n \mid 2d^n b_1^n$, whence $a_1^n \mid 2b_1^n$ and by the use of $(a_1^n, b_1^n) = 1$ and Theorem 5 we have $a_1^n \mid 2$, which since $n > 1$, implies $a_1 = 1$, and consequently $a = d$, which gives $a \mid b$. □

THEOREM 7. *If a natural number is the m-th power of a rational number and m is natural, then it is the m-th power of a natural number.*

PROOF. Suppose that a natural number n is the mth power of a rational number p/q. As we know from § 4, we may assume that p and q are natural numbers and that $(p, q) = 1$. Hence, by Theorem 6^a, we infer that $(p^m, q) = 1$. On the other hand, by $n = (p/q)^m$, we have $nq^m = p^m$, whence $q \mid p^m$ and therefore $q \mid (p^m, q) = 1$. Thus $q = 1$ (since q is a natural number), and consequently, $n = p^m$, which means that n is the mth power of a natural number. □

As an immediate consequence of Theorem 7 we have the following

Corollary. *The m-th root of a natural number which is not the m-th power of a natural number is an irrational number.*

In particular, the numbers $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{10}$, $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\sqrt[3]{4}$ are irrational.

Exercises. 1. Prove that if a, b, d are integers such that $(a, b) = 1$ and $d \mid a+b$, then $(d, a) = 1$ and $(d, b) = 1$.

Proof. Suppose that $(a,b) = 1$ and $d \mid a+b$. If $(d,a) = \delta$, then $\delta \mid d$ and $\delta \mid a$, whence, since $d \mid a+b$, $\delta \mid a+b$ and consequently $\delta \mid (a+b)-a$, which gives $\delta \mid b$. Thus $\delta \mid (a,b)$. Hence $\delta = (d,a) = 1$. The proof of the equality $(d,b) = 1$ is analogous. ☐

2. Prove that if n, n_1 and n_2 are natural numbers, $n \mid n_1 n_2$ and none of the numbers n_1, n_2 is divisible by n, then the number

$$(*) \qquad d = \frac{n_1}{\left(n_1, \dfrac{n_1 n_2}{n}\right)}$$

is a divisor of the number n, and moreover $1 < d < n$.

Proof. In virtue of $(*)$ we have $\dfrac{n_1}{d} = \left(n_1, \dfrac{n_1 n_2}{n}\right)$. Thus the number $\dfrac{n_1}{d}$ is natural and, consequently $n_1 = \dfrac{n_1}{d} k$, $\dfrac{n_1 n_2}{n} = \dfrac{n_1}{d} l$, where k and l are relatively prime natural numbers. We also have $k = d, n_2 d = nl$ and, since $(d, l) = 1$, $d \mid n$. Thus d is a divisor of the number n. If $d = 1$, then we would have $n_2 = nl$ and consequently $n \mid n_2$, contrary to the assumption. If $d = n$, then, since, by $(*)$, $d \mid n_1$, we have $n \mid n_1$, which also contradicts the assumption. Thus d is a divisor of n for which $1 < d < n$, as required.

3. Prove that if a and b are two relatively prime natural numbers and m is an arbitrary natural number, then in the arithmetical progression $a+bk$ $(k = 0, 1, 2, \ldots)$ there are infinitely many numbers relatively prime to m.

Proof. Suppose $(a, b) = 1$ and m is an arbitrary natural number. The number m is, clearly, divisible by some divisors that are relatively prime to a, e.g. the number 1. Let c denote the greatest one of them. We are going to prove that the number $a + bc$ is relatively prime to m. We have $(a, b) = 1$, and, according to the definition of $c, (a, c) = 1$. Hence $(a, bc) = 1$. From Exercise 1 it follows that if $d \mid a+bc$, then $(d, a) = 1$ and $(d, bc) = 1$; thus, a fortiori, $(d, c) = 1$. On the other hand, if also $d \mid m$, then since $c \mid m$ and $(d, c) = 1$, by the corollary to Theorem 5 we have $dc \mid m$. Further, since $(d, a) = 1$ and $(a, c) = 1$, the equality $(a, dc) = 1$ holds. Thus the number dc is a divisor of the number m and is relatively prime to a, but, since c is the greatest divisor having these properties, $d = 1$. So far we have proved that if d is a common divisor of the numbers $a+bc$ and m, then $d = 1$; this proves that $(a+bc, m) = 1$. From this relation we conclude that if l is an arbitrary natural number, then for $k = c+lm$ the numbers $a+bk$ and m are relatively prime, and this is what we had to prove. ☐

4. Prove that if a and b are relatively prime natural numbers then the arithmetical progression $a+kb(k = 0,1,2,...)$ contains an infinite subsequence such that any two numbers of the subsequence are relatively prime.

PROOF. We define the required subsequence $u_1, u_2, \ldots$ inductively. Let $u_1 = a$. Now, let n be an arbitrary natural number. Suppose we have already defined the numbers $u_1, u_2, \ldots, u_n$ and that any two of them are relatively prime. In virtue of Exercise 3, for the natural number $u_1 u_2 \ldots u_n$ there is a term of the progression $a+kb(k = 0,1,2,\ldots)$ which is relatively prime to $u_1 u_2 \ldots u_n$. Let us denote it by u_{n+1}. It is readily shown that the sequence $u_1, u_2, \ldots$ defined in this way has the desired properties. ☐

THEOREM 8. *Suppose that a and b are two relatively prime natural numbers such that the product of them is the n-th power of a natural number, i.e.* $ab = c^n$, *where n is a natural number. Then the numbers a and b are themselves the n-th powers of natural numbers.*

PROOF. Let $(a,c) = d$. Then $a = da_1$, $c = dc_1$, where $(a_1, c_1) = 1$. By the assumption that $ab = c^n$, we have $da_1 b = d^n c_1^n$, whence $a_1 b = d^{n-1} c_1^n$. But in view of $d \mid a$ and $(a,b) = 1$, we obtain $(d,b) = 1$, whence, by Theorem 6^a, we obtain $(d^{n-1}, b) = 1$. The equality $a_1 b = d^{n-1} c_1^n$ implies the relation $b \mid d^{n-1} c_1^n$. Therefore, by Theorem 5, $b \mid c_1^n$. On the other hand, since $(a_1, c_1) = 1$, Theorem 6^a implies that $(a_1, c_1^n) = 1$ and, since the equality $a_1 b = d^{n-1} c_1^n$ gives the relation $c_1^n \mid a_1 b$, then, by Theorem 5, we obtain $c_1^n \mid b$. The relations $b \mid c_1^n$ and $c_1^n \mid b$ together imply the equality $b = c_1^n$, whence $a_1 = d^{n-1}$ and $a = da_1 = d^n$. Thus we arrive at the final conclusion that each of the numbers a and b is the nth power of a natural number. ☐

COROLLARY. *Suppose that k, c and n are natural numbers, that* $a_1, a_2, \ldots, a_k$ *is a sequence of natural numbers such that any two of them are relatively prime and that* $a_1 a_2 \ldots a_k = c^n$. *Then every number of the sequence* $a_1, a_2, \ldots, a_k$ *is the n-th power of a natural number.*

7. Proof of the formulae $(a_1, a_2, \ldots, a_{n+1}) = ((a_1, a_2, \ldots, a_n), a_{n+1})$ and $[a_1, a_2, \ldots, a_{n+1}] = [[a_1, a_2, \ldots, a_n], a_{n+1}]$

We are going to prove the formulae

$$(a_1, a_2, \ldots, a_{n+1}) = ((a_1, a_2, \ldots, a_n), a_{n+1}) \tag{2}$$

$$[a_1, a_2, \ldots, a_{n+1}] = [[a_1, a_2, \ldots, a_n], a_{n+1}]. \tag{3}$$

THEOREM 9. *For natural numbers* $n > 2$ *and* $a_1, a_2, \ldots, a_{n+1}$ *formula* (2) *holds.*

PROOF. Let $d = ((a_1, a_2, \dots, a_n), a_{n+1})$. Then d is a common divisor of the numbers $(a_1, a_2, \dots, a_n)$ and a_{n+1}. Since $(a_1, a_2, \dots, a_n)$ is a divisor of each of the numbers $a_1, a_2, \dots, a_n, d$ must be a divisor of each of the numbers $a_1, a_2, \dots, a_n, a_{n+1}$. Now let d' denote an arbitrary divisor of the numbers $a_1, a_2, \dots, a_n, a_{n+1}$. In virtue of Theorem 2, we have $d' \mid (a_1, a_2, \dots, a_n)$. Since also $d' \mid a_{n+1}$, we have, by the definition of the number d and again by Theorem 2, $d' \mid d$. Thus d is a common divisor of the numbers $a_1, a_2, \dots, a_n, a_{n+1}$, which is divisible by every common divisor of these numbers. Consequently, d is the greatest common divisor of $a_1, a_2, \dots, a_{n+1}$. Formula (2) is thus proved. □

It follows that in order to find the number $(a_1, a_2, \dots, a_n)$ we may calculate the divisors $d_2 = (a_1, a_2)$, $d_3 = (d_2, a_3)$, $d_4 = (d_3, a_4), \dots, d_{n-1} = (d_{n-1}, a_{n-1})$, and $(a_1, a_2, \dots, a_n) = (d_{n-1}, a_n)$, successively.

Thus the calculation of the greatest common divisor of arbitrarily many numbers reduces to the successive calculation of the greatest common divisor of two numbers.

THEOREM 10. *For natural numbers* $n \geqslant 2$ *and* $a_1, a_2, \dots, a_{n+1}$ *formula* (3) *holds.*

PROOF. Let $N = [[a_1, a_2, \dots, a_n], a_{n+1}]$. Then N is a common multiple of the numbers $[a_1, a_2, \dots, a_n]$ and a_{n+1}. Since $[a_1, a_2, \dots, a_n]$ is a multiple of each of the numbers, $a_1, a_2, \dots, a_n$, the number N is a multiple of each of the numbers $a_1, a_2, \dots, a_n, a_{n+1}$. Let M denote an arbitrary common multiple of the numbers $a_1, a_2, \dots, a_n, a_{n+1}$. In virtue of Theorem 1, we have $[a_1, a_2, \dots, a_n] \mid M$. Since also $a_{n+1} \mid M$, we have again by Theorem 1, $[[a_1, a_2, \dots, a_n], a_{n+1}] \mid M$ or, equally, $N \mid M$. Thus N is a common multiple of the numbers $a_1, a_2, \dots, a_n, a_{n+1}$ which is a divisor of every common multiple of these numbers. Consequently, N is their least common multiple. This completes the proof of formula (3). □

It follows that in order to find the number $[a_1, a_2, \dots, a_n]$ we may calculate $N_2 = [a_1, a_2]$, $N_3 = [N_2, a_3], \dots, N_{n-1} = [N_{n-2}, a_{n-1}]$ and $[a_1, a_2, \dots, a_n] = [N_{n-1}, a_n]$ successively.

THEOREM 11. *If* n *is a natural number* $\geqslant 2$ *and if any two of the natural numbers* $a_1, a_2, \dots, a_n$ *are relatively prime, then* $[a_1, a_2, \dots, a_n] = a_1 a_2 \dots a_n$.

PROOF. In virtue of the corollary to Theorem 4, Theorem 11 is true for $n = 2$. Now, let n be an arbitrary natural number $\geqslant 2$. Suppose that the theorem is true for the natural number n and that $a_1, a_2, \ldots, a_n, a_{n+1}$ are natural numbers such that any two of them are relatively prime. Consequently, $(a_i, a_{n+1}) = 1$ for all $i = 1, 2, \ldots, n$. Hence, by Theorem 6[a] and corollary to Theorem 4, $[a_1 a_2 \ldots a_n, a_{n+1}] = a_1 a_2 \ldots a_n a_{n+1}$. But by the hypothesis, Theorem 11 is true for the number n; hence $a_1 a_2 \ldots a_n = [a_1, a_2, \ldots, a_n]$, and in virtue of (3),

$$a_1 a_2 \ldots a_n a_{n+1} = [[a_1, a_2, \ldots, a_n], a_{n+1}] = [a_1, a_2, \ldots, a_n, a_{n+1}],$$

which proves the theorem for the number $n+1$, and thus, by induction, the theorem holds for all natural numbers. ☐

It is worth-while to note that the implication stated by Theorem 11 could be reversed: if for $n \geqslant 2$ and natural numbers $a_1, a_2, \ldots, a_n$ the formula $[a_1, a_2, \ldots, a_n] = a_1 a_2 \ldots a_n$ holds, then any two of the numbers $a_1, a_2, \ldots, a_n$ are relatively prime.

One can also prove the following statement: In order that the product of $n > 2$ natural numbers be equal to the product of their greatest common divisor and their least common multiple it is necessary and sufficient that any two of those numbers be relatively prime.

This statement, however, is not true for $n = 2$, since for instance the numbers 2 and 4 are not relatively prime and $2 \cdot 4 = (2, 4) \cdot [2, 4]$.

8. Rules for calculating the greatest common divisor of two numbers.

Let a and b be two given natural numbers. The process of dividing the number a by b yields the quotient q and the remainder r less than b. We have

$$a = qb + r.$$

It follows immediately from this equality that every common divisor of the numbers a and b is a divisor of the remainder $r = a - qb$, and that every common divisor of the numbers b and r is a divisor of the number a. Therefore the common divisors of a and b are the same as the common divisors of b and r. So

$$(a, b) = (b, r).$$

We adopt the notation $a = n_0$, $b = n_1$, $r = n_2$, and write the above equality as

$$(n_0, n_1) = (n_1, n_2).$$

If $n_2 = 0$, then clearly, $(n_0, n_1) = n_1$. If, however, $n_2 \neq 0$, then we can divide n_1 by n_2 and denote the remainder by n_3; again

$$(n_1, n_2) = (n_2, n_3).$$

Proceeding in this way we obtain the following sequence of equalities:

$$\begin{aligned}(n_0, n_1) &= (n_1, n_2),\\ (n_1, n_2) &= (n_2, n_3),\\ (n_2, n_3) &= (n_3, n_4),\\ &\ldots\ldots\ldots\ldots\\ (n_{k-2}, n_{k-1}) &= (n_{k-1}, n_k),\\ (n_{k-1}, n_k) &= (n_k, n_{k+1}).\end{aligned} \tag{4}$$

Since n_{i+1} denotes here the remainder given by the division of n_{i-1} by n_i $(i = 1, 2, \ldots, k)$, we have $n_{i+1} < n_i$ for $i = 1, 2, \ldots, k$. Therefore the n_i's are continually decreasing, i.e.

$$n_1 > n_2 > n_3 > \ldots \geqslant 0.$$

This sequence cannot be infinite, since there are only n different non-negative integers less than n. Hence in the sequence of equalities (4) there exists a last one, say $(n_{k-1}, n_k) = (n_k, n_{k+1})$. If we could have $n_{k+1} \neq 0$, then we would divide n_k by n_{k+1} and obtain another equality, $(n_k, n_{k+1}) = (n_{k+1}, n_{k+2})$, contrary to the assumption that there are only k equalities in sequence (4). Thus $n_{k+1} = 0$, and consequently $(n_{k-1}, n_k) = n_k$. Accordingly, equalities (4) imply

$$(n_0, n_1) = (n_1, n_2) = (n_2, n_3) = \ldots = (n_{k-1}, n_k) = n_k,$$

whence

$$(n_0, n_1) = n_k.$$

From the above reasoning we may deduce the following rule for finding the greatest common divisor of two given natural numbers:

In order to find the greatest common divisor of two given natural numbers n_0 and n_1 we divide n_0 by n_1 and find the remainder n_2. Then we divide n_1 by n_2 and again find the remainder n_3. Continuing, we divide n_2 by n_3 and so on. At the final step we obtain a remainder which is equal to zero. The remainder obtained in the last but one step is the greatest common divisor of the numbers n_0 and n_1.

The rule we have just presented is called either the *division algorithm*, the *Euclidean algorithm*, or the *algorithm of continued fractions*. The last name will find its justification in §9.

It follows from the Euclidean algorithm that the greatest common divisor of two given natural numbers can be obtained in finitely many divisions.

The number of the divisions, however, can be arbitrarily large for suitably chosen natural numbers a and b. As a matter of fact, *for each natural number n there exist natural numbers a_n and b_n such that in order to find their greatest common divisor by means of the Euclidean algorithm n divisions are needed.*

We prove this by providing ourselves with the sequence

$$(5) \qquad u_1 = u_2 = 1, \qquad u_n = u_{n-1} + u_{n-2}, \qquad \text{where} \qquad n = 3, 4, \ldots$$

We have

$$(6) \quad u_1 = 1, \quad u_2 = 1, \quad u_3 = 2, \quad u_4 = 3, \quad u_5 = 5, \quad u_6 = 8, \quad u_7 = 13, \quad u_8 = 21, \quad u_9 = 34, \ldots$$

This is the *Fibonacci sequence*: its first two terms are equal to 1 and each of the following terms is the sum of the preceding two.

Let $a_n = u_{n+2}$, $b_n = u_{n+1}$. We apply the Euclidean algorithm to find the number $(a_n, b_n) = (u_{n+2}, u_{n+1})$. We obtain the following sequence of divisions:

$$\begin{aligned} u_{n+2} &= 1 \cdot u_{n+1} + u_n, \\ u_{n+1} &= 1 \cdot u_n + u_{n-1}, \\ &\cdots\cdots\cdots\cdots \\ u_4 &= 1 \cdot u_3 + u_2, \\ u_3 &= 2 \cdot u_2. \end{aligned}$$

Evidently the number of necessary divisions is n. For example, in order to find the greatest common divisor of the numbers $u_{12} = 144$ and $u_{11} = 89$ by means of the Euclidean algorithm one needs 10 divisions.

It can easily be proved that the least numbers for which one needs exactly n divisions to find their greatest common divisor by means of the Euclidean algorithm are the numbers u_{n+2} and u_{n+1}.

We now prove the following

THEOREM 12. *The number of divisions necessary to find the greatest common divisor of two natural numbers by means of the Euclidean algorithm is not greater than 5 multiplied by the number of digits in the decimal expansion of the smaller of the numbers* (Lamé [1]).

PROOF. First we prove the following property of the Fibonacci sequence u_n $(n = 1, 2, \ldots)$ defined above:

$$u_{n+5} > 10u_n \quad \text{for} \quad n = 2, 3, \ldots \tag{7}$$

A straightforward computation shows that for $n = 2$ formula (7) holds (for, $u_7 = 13 > 10u_2 = 10$). Further, let $n \geqslant 3$. In virtue of (5) we have

$$\begin{aligned} u_{n+5} &= u_{n+4} + u_{n+3} = 2u_{n+3} + u_{n+2} = 3u_{n+2} + 2u_{n+1} \\ &= 5u_{n+1} + 3u_n = 8u_n + 5u_{n-1} . \end{aligned}$$

Since the sequence (6) is not decreasing, $u_n = u_{n-1} + u_{n-2} \leqslant 2u_{n-1}$, whence $2u_n \leqslant 4u_{n-1}$ and therefore $u_{n+5} = 8u_n + 5u_{n-1} > 8u_n + 4u_{n-1} \geqslant 10u_n$, which implies $u_{n+5} > 10u_n$, as required.

From (7), by a simple induction, we obtain

$$u_{n+5l} > 10^l u_n , \qquad n = 2, 3, \ldots ; \; l = 1, 2, \ldots \tag{8}$$

Now, let n_0 and $n_1 < n_0$ be two given natural numbers. Suppose that in order to find the greatest common divisor (n_0, n_1) by means of the Euclidean algorithm the following k divisions are necessary:

$$\begin{aligned} n_0 &= q_1 n_1 + n_2 , \\ n_1 &= q_2 n_2 + n_3 , \\ &\cdots\cdots\cdots\cdots \\ n_{k-2} &= q_{k-1} n_{k-1} + n_k , \\ n_{k-1} &= q_k n_k . \end{aligned} \tag{9}$$

We have, of course $q_k \geqslant 2$, since for $q_k = 1$ we would have $n_k = n_{k-1}$, which is impossible because n_k is the remainder obtained by dividing n_{k-2} by n_{k-1}. Thus $n_{k-1} = q_k n_k \geqslant 2n_k \geqslant 2 = u_3$. Hence $n_{k-2} \geqslant n_{k-1} + n_k \geqslant u_3 + u_2 = u_4$, $n_{k-3} \geqslant n_{k-2} + n_{k-1} \geqslant u_4 + u_3 = u_5, \ldots, n_1 \geqslant u_{k+1}$. So, if $k > 5l$ or equivalently, $k \geqslant 5l + 1$, then $n_1 \geqslant u_{5l+2}$ and, by (8) (with $n = 2$), $n_1 > 10^l$. This means, however, that n_1 has at least $l + 1$ digits in the scale of ten. Thus if n_1 has l digits, then $k \leqslant l$, which shows the truth of Theorem 12. □

It follows from Theorem 12 that in order to find by means of the Euclidean algorithm the greatest common divisor of two natural numbers the smaller of which has at most 6 digits at most 30 divisions are needed. We note that in Theorem 12 the number 5 cannot be replaced by the number 4 since, as we have seen, we need 10 divisions in order to find the greatest common divisor of 144 and 89 (cf. Brown J. L. Jr. [1], Dixon [1], [2]).

9. Representation of rationals as simple continued fractions.

Let n_0, n_1 be two given natural numbers, and (9) the sequence of equalities obtained by the repeated application of the Euclidean algorithm to the numbers n_0 and n_1. For all $i = 1, 2, ..., k-1$ we have

$$\frac{n_{i-1}}{n_i} = q_i + \cfrac{1}{\cfrac{n_i}{n_{i+1}}} \quad \text{and} \quad \frac{n_{k-1}}{n_k} = q_k,$$

whence

$$\frac{n_0}{n_1} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}, \tag{10}$$

which we write in the abbreviated form

$$\frac{n_0}{n_1} = q_1 + \frac{1|}{|q_2} + \frac{1|}{|q_3} + \frac{1|}{|q_4} + \ldots + \frac{1\ |}{|q_{k-1}} + \frac{1|}{|q_k}.$$

In formulae (9) q_1 is a positive integer which is the quotient obtained by dividing the natural number n_0 by the natural number n_1, the numbers q_i, for $i = 2, 3, ..., k$, are natural numbers, since $n_{i-1} > n_i$. The expression on the right-hand side of formula (10), q_1 being an integer and $q_2, q_3, ..., q_n$ being natural numbers, is called a *simple continued fraction.*

Thus we may say that by the use of the Euclidean algorithm every rational number can be represented as a simple continued fraction.

EXAMPLES. Consider the number 314159/100000. The successive application of the Euclidean algorithm gives

$$\begin{aligned}
314159 &= 3\cdot 100000 + 14159,\\
100000 &= 7\cdot 14159 + 887,\\
14159 &= 15\cdot 887 + 854,\\
887 &= 1\cdot 854 + 33,\\
854 &= 25\cdot 33 + 29,\\
33 &= 1\cdot 29 + 4,\\
29 &= 7\cdot 4 + 1,\\
4 &= 4\cdot 1.
\end{aligned}$$

Thus

$$\frac{314159}{100000} = 3 + \frac{1|}{|7} + \frac{1|}{|15} + \frac{1|}{|1} + \frac{1|}{|25} + \frac{1|}{|1} + \frac{1|}{|7} + \frac{1|}{|4}.$$

To take another example, consider the number u_{n+1}/u_n, where u_k ($k = 1, 2, \ldots$) denotes the Fibonacci sequence (cf. § 8). It follows immediately from (10) that for all natural numbers n we have

$$\frac{u_{n+1}}{u_n} = 1 + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \ldots + \frac{1|}{|1},$$

where the sign $\frac{\;|}{|\;}$ appears $n-1$ times. Thus, e.g.

$$\frac{u_2}{u_1} = 1, \quad \frac{u_3}{u_2} = 1 + \frac{1|}{|1}, \quad \frac{u_4}{u_3} = 1 + \frac{1|}{|1} + \frac{1|}{|1}$$

and so on. We could, of course, have also written

$$\frac{u_4}{u_3} = 1 + \frac{1|}{|2}.$$

We shall go into some more details concerning continued fractions in Chapter VIII.

10. Linear form of the greatest common divisor

THEOREM 13. *If $a_1, a_2, \ldots, a_m$ are $m > 1$ integers such that at least one of them is different from zero, then there exist integers $t_1, t_2, \ldots, t_m$ such that*

$$(a_1, a_2, \ldots, a_m) = a_1 t_1 + a_2 t_2 + \ldots + a_m t_m. \tag{11}$$

PROOF. Denote by D the set of the natural numbers defined by the rule: a number n belongs to the set D if and only if there exist integers $x_1, x_2, \ldots, x_m$ such that

$$n = a_1 x_1 + a_2 x_2 + \ldots + a_m x_m. \tag{12}$$

In other words, D is the set of all natural numbers of the form $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$, where $x_1, x_2, \ldots, x_m$ are integers.

The set D is non-empty (i.e. it contains at least one number) since if, say, $a_k \neq 0$ (where $1 \leqslant k \leqslant m$) then $|a_k|$ belongs to D because it is plainly of the form $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$, where $x_i = 0$ for $i \neq k$ and x_k equals $+1$ or -1 depending on whether $a_k > 0$ or $a_k < 0$.

Denote by d the least natural number belonging to the set D. (The number d does exist since every set of natural numbers contains the least one.) If d belongs to the set D, then, by definition, there exist integers $t_1, t_2, \ldots, t_m$ such that

$$d = a_1 t_1 + a_2 t_2 + \ldots + a_m t_m. \tag{13}$$

But since d is the least number of the set D, for every natural number n of the form (12), where $x_1, x_2, \ldots, x_m$ are integers, the inequality $n \geqslant d$ holds.

We are going to prove that for arbitrary integers $x_1, x_2, \ldots, x_m$ the number $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$ is divisible by d. Suppose that this is not the case. Then, for some integers $y_1, y_2, \ldots, y_m$ the division of the number $a_1 y_1 + a_2 y_2 + \ldots + a_m y_m$ by d yields a quotient q and a positive remainder r. We have $a_1 y_1 + a_2 y_2 + \ldots + a_m y_m = qd + r$, whence, by (13), $r = a_1 y_1 + a_2 y_2 + \ldots + a_m y_m - q(a_1 t_1 + a_2 t_2 + \ldots + a_m t_m) = a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$, where $x_i = y_i - qt_i$ are, of course, integers for all $i = 1, 2, \ldots, m$. Thus the natural number r is of the form (12), which implies that r belongs to the set D. But, on the other hand, r, as the remainder obtained by dividing an integer by d, is less than d, contrary to the assumption that d was the least number belonging to the set D.

We have thus proved that for arbitrary integers $x_1, x_2, \ldots, x_m$ the number $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$ is divisible by d. Hence, in particular, $d \mid a_1 x_1 + a_2 x_2 + \ldots + a_m x_m$, where $x_k = 1$ and $x_i = 0$ for $i \neq k$. Hence, for each $k = 1, 2, \ldots, m$, $d \mid a_k$, which means that d is a common divisor of the numbers $a_1, a_2, \ldots, a_m$.

Now, let δ denote an arbitrary common divisor of the numbers $a_1, a_2, \ldots, a_m$, and let $z_1, z_2, \ldots, z_m$ be the integers for which $a_k = \delta z_k$ $(k = 1, 2, \ldots, m)$. Hence, by (13), we have

$$d = a_1 t_1 + a_2 t_2 + \ldots + a_m t_m = (t_1 z_1 + t_2 z_2 + \ldots + t_m z_m)\delta,$$

whence $\delta \mid d$. From this we conclude that the common divisor d is equal to $(a_1, a_2, \ldots, a_m)$ because it is divisible by every common divisor of the numbers $a_1, a_2, \ldots, a_m$. Thus (13) implies (11), and this completes the proof of the theorem. ☐

Let $a_1, a_2, \ldots, a_m$ be $m > 1$ integers such that $(a_1, a_2, \ldots, a_m) = 1$. By Theorem 13 there exist integers $t_1, t_2, \ldots, t_m$ such that

$$a_1 t_1 + a_2 t_2 + \ldots + a_m t_m = 1. \tag{14}$$

Conversely, suppose that for given integers $a_1, a_2, \ldots, a_m$ there exist integers $t_1, t_2, \ldots, t_m$ such that equation (14) holds. The left-hand side of the equation is clearly divisible by every common divisor of the numbers $a_1, a_2, \dots, a_m$. But, since the right-hand side of the equation is 1, we see that $(a_1, a_2, \dots, a_m) = 1$, and this proves the following theorem.

THEOREM 14. *For $m > 1$ the relation $(a_1, a_2, \dots, a_m) = 1$ holds if and only if there exist integers $t_1, t_2, \dots, t_m$ such that $a_1 t_1 + a_2 t_2 + \dots + a_m t_m = 1$.*

COROLLARY. *If for integers d, k and $a_1, a_2, \dots, a_m$ with $m > 1$ we have $(a_1, a_2, \dots, a_m) = 1$ and $d \mid ka_i$ with $i = 1, 2, \dots, m$, then $d \mid k$.*

PROOF. By Theorem 14, since $(a_1, a_2, \dots, a_m) = 1$, there exist integers $t_1, t_2, \dots, t_m$ such that $a_1 t_1 + a_2 t_2 + \dots + a_m t_m = 1$. But since $d \mid ka_i$ for all $i = 1, 2, \dots, m$, $d \mid ka_i t_i$ for $i = 1, 2, \dots, m$, whence we infer that $d \mid k(a_1 t_1 + a_2 t_2 + \dots + a_m t_m)$ and, consequently, $d \mid k$, as required. □

We note that theorems analogous to Theorem 13 and 14 are valid for polynomials of one variable, and fail for polynomials of several variables. In fact, if $f(x, y) = x$ and $g(x, y) = y$, then the greatest common divisor of the polynomials $f(x, y)$ and $g(x, y)$ is a constant. The expression $xp(x, y) + yq(x, y)$, however, cannot be a constant different from zero whichever polynomials $p(x, y), q(x, y)$ are taken (Bochner [1]).

Let us return for a while to Theorem 13. It would be of some interest to find for given numbers $a_1, a_2, \dots, a_m$ the numbers $t_1, t_2, \dots, t_m$ for which (11) holds. The proof of the theorem does not contain any hint how to do this. (We say that it is *purely an existential proof.*) We can do this, however, with the aid of the Euclidean algorithm. We start with the case $m = 2$. Then, apart from the trivial case when one of the numbers is equal to zero, we change, if necessary, the signs of t_1 and t_2 and assume that a_1 and a_2 are natural numbers, which we denote by n_0 and n_1, respectively. Applying the Euclidean algorithm to them we obtain formulae (9). As we know, $n_k = (n_0, n_1)$. The last but one equality of (9) is equivalent to

$$n_k = n_{k-2} - q_{k-1} n_{k-1}. \tag{15}$$

Substituting here the value of n_{k-1} obtained from the last but two equality of (9), we have

$$\begin{aligned} n_k &= n_{k-2} - q_{k-1}(n_{k-3} - q_{k-2} n_{k-2}) \\ &= -q_{k-1} n_{k-3} + (1 + q_{k-1} q_{k-2}) n_{k-2}. \end{aligned}$$

Further, we substitute in the last equality the value of n_{k-2} obtained from the equality last but three of (9) and so on. Proceeding in this way, we arrive after $k-2$ substitutions at the equality $n_k = n_0 x + n_1 y$, where x

and y are integers. It is obvious that this process leads us to an effective calculation of the numbers $x = t_1$ and $y = t_2$.

In the general case, when m is an arbitrary natural number > 1, we proceed by induction. Suppose that for all integers $a_1, a_2, \ldots, a_m$ we have a rule for finding the numbers $t_1, t_2, \ldots, t_m$ satisfying equality (11). Let $a_1, a_2, \ldots, a_m, a_{m+1}$ be given integers. By Theorem 9 we have $(a_1, a_2, \ldots, a_{m+1}) = \big((a_1, a_2, \ldots, a_m), a_{m+1}\big)$. As we know from the reasoning above, there is a rule for finding the numbers x and y satisfying the equality

$$\big((a_1, a_2, \ldots, a_m), a_{m+1}\big) = (a_1, a_2, \ldots, a_m)\, x + a_{m+1}\, y. \tag{16}$$

We set $x_i = t_i x$ for $i = 1, 2, \ldots, m$ and $x_{m+1} = y$. In virtue of (16) and (11) we have

$$(a_1, a_2, \ldots, a_{m+1}) = a_1 x_1 + a_2 x_2 + \ldots + a_m x_m + a_{m+1} x_{m+1}, \tag{17}$$

where $x_1, x_2, \ldots, x_{+1}$ are integers. Thus we have established a rule for finding integers $x_1, x_2, \ldots, x_{m+1}$ satisfying equation (17) provided that a rule for finding integers $t_1, t_2, \ldots, t_m$ is given.

This, by induction, completes the proof of the following assertion: *for every $m > 1$ and integers $a_1, a_2, \ldots, a_m$ such that at least one of them is different from zero there exists a rule for finding integers $t_1, t_2, \ldots, t_m$ satisfying equation* (11).

11. Indeterminate equations of *m* variables and degree 1

THEOREM 15. *Given $m > 1$ integers $a_1, a_2, \ldots, a_m$ at least one of which is different from zero. The aquation*

$$a_1 x_1 + a_2 x_2 + \ldots + a_m x_m = b, \tag{18}$$

is solvable in integers $x_1, x_2, \ldots, x_m$ if and only if $(a_1, a_2, \ldots, a_m) \mid b$.

PROOF. Suppose that there exist integers $x_1, x_2, \ldots, x_m$ satisfying equation (18). It follows immediately from (18) that every common divisor of the numbers $a_1, a_2, \ldots, a_m$ is a divisor of the number b. Thus $(a_1, a_2, \ldots, a_m) \mid b$, and this proves the necessity of the condition.

On the other hand, suppose that $d = (a_1, a_2, \ldots, a_m) \mid b$. Then there exists an integer k such that $b = kd$. Since at least one of the numbers $a_1, a_2, \ldots, a_m$ is different from zero, then, by Theorem 13, there exist integers $t_1, t_2, \ldots, t_m$ satisfying equation (11). Set $x_i = kt_i$ for all i

$= 1, 2, \ldots, m$. Hence, since $d = (a_1, a_2, \ldots, a_m)$, in virtue of formula (11), we have

$$a_1 x_1 + a_2 x_2 + \ldots + a_m x_m = k(a_1 t_1 + a_2 t_2 + \ldots + a_m t_m) = kd = b.$$

Thus the condition of Theorem 15 is sufficient. ☐

Theorem 15 can also be expressed in the following form:

In order that an equation of degree 1 *with integral coefficients and* $m > 1$ *variables be solvable in integers, it is necessary and sufficient that the constant term of the equation be divisible by the greatest common divisor of the coefficients at the variables.*

From the proof of Theorem 15 and the fact that for given integers $a_1, a_2, \ldots, a_m$ we can effectively find integers $t_1, t_2, \ldots, t_m$ satisfying equation (11), it follows that if equation (11) is solvable in integers, then also we can effectively find integers $x_1, x_2, \ldots, x_m$ satisfying equation (11), i.e. we have a rule for finding at least one of the integral solutions of equation (18). The question arises what is the rule for finding all the integral solutions of equation (18).

We start with the case $m = 2$. Consider an equation

$$ax + by = c, \tag{19}$$

where a, b, c are integers and $(a, b) \mid c$. We may assume that both a and b are different from zero, since otherwise we would have an equation in one variable, for which we could easily find the solution. Since $(a, b) \mid c$, we can find integers x_0, y_0 such that

$$ax_0 + by_0 = c. \tag{20}$$

Suppose now that x and y are arbitrary integers satisfying equation (19). From equalities (19) and (20) we derive

$$a(x - x_0) = b(y_0 - y). \tag{21}$$

Since $d = (a, b)$ is the greatest common divisor of the numbers a and b, we have $a = da_1$, $b = db_1$, where a_1 and b_1 are relatively prime integers. From (21) we have

$$a_1(x - x_0) = b_1(y_0 - y). \tag{22}$$

Hence, by $(a_1, b_1) = 1$ and Theorem 6, we have $b_1 \mid x - x_0$, whence $x - x_0 = b_1 t$, where t is an integer. By (22), $a_1 b_1 t = b_1(y_0 - y)$, whence, since $b_1 \neq 0$, we obtain $y_0 - y = a_1 t$. The equalities $x - x_0 = b_1 t$, $y_0 - y = a_1 t$ imply

$$x = x_0 + b_1 t, \qquad y = y_0 - a_1 t. \tag{23}$$

We have thus proved that if x, y form an integral solution of equation (19), then they can be written in the form (23), where t is an integer.

Now, let t denote an arbitrary integer. We find x and y from (23) and calculate the value of

$$ax+by = a(x_0+b_1 t)+b(y_0-a_1 t) = ax_0+by_0+(ab_1-ba_1)t.$$

Hence, in virtue of (20) and the identity $ab_1-ba_1 = da_1 b_1 - db_1 a_1 = 0$ we obtain equality (19). Thus,

In order that integers x and y constitute a solution of equation (19) *it is necessary and sufficient that for some natural t formulae* (23) *hold.*

It follows that for $t = 0, \pm 1, \pm 2, \ldots$ formulae (23) give all the integral solutions of equation (19). Since at least one of the numbers a_1, b_1 is different from zero, if equation (19) has at least one integral solution, then it has infinitely many of them.

We now prove the following

THEOREM 16. *If a and b are relatively prime natural numbers, then there exist natural numbers u and v such that $au-bv = 1$.*

PROOF. In virtue of Theorem 15 there exist integers x_0 and y_0 such that $ax_0+by_0 = 1$. We choose an integer t_0 such that $t_0 > x_0/b$ and $t_0 > y_0/a$, and put $u = x_0+bt_0 > 0$ and $v = -(y_0-at_0) > 0$. Plainly, u and v are natural numbers and $au-bv = ax_0+by_0 = 1$. ☐

From Theorem 16 we derive the following three corollaries.

COROLLARY 1. *If natural numbers a, b, l, m satisfy the onditions*

then there exists a natural number n such that $a = n^m$ and $b = n^l$.

PROOF. Since $(l, m) = 1$, then, in virtue of Theorem 16, there exist natural numbers r and s such that $lr-ms = 1$. Hence, since $a^l = b^m$, we have $a = a^{lr-ms} = a^{lr}/a^{ms} = (b^r/a^s)^m$. The number a is then the mth power of a rational number b^r/a^s, which, in virtue of Theorem 7, implies that it is the m-th power of a natural number $n = b^r/a^s$. Thus $a = n^m$, whence $b^m = a^l = n^{ml}$, which shows that $b = n^l$. This gives $a = n^m$ and $b = n^l$, where n is a natural number as required. ☐

COROLLARY 2. *If a and b are two relatively prime natural numbers, then every natural number $n > ab$ can be written in the form $n = ax+by$, where x, y are natural numbers.*

PROOF. Let a and b be two relatively prime natural numbers, and u, v natural numbers satisfying Theorem 16. We then have $au-bv = 1$, whence, for $n > ab$, $anu-bnv = n > ab$, and, consequently, $nu/b-$ $-nv/a > 1$. Therefore there exists an integer t such that $nv/a < t < nu/b$. (Such is the greatest integer less that nu/b.) Let $x = nu-bt$, $y = at-nv$. We have $x > 0$ and $y > 0$ and also $ax+by = a(nu-bt)+b(at-nv) = n$, which completes the proof of Corollary 2. ☐

We notice that in Corollary 2 the number ab cannot be replaced by a smaller number. The reason is that if $(a, b) = 1$, the number ab itself does not have a representation in the form $ax+by = ab$ where x, y are natural numbers. In fact, suppose $ab = ax+by$, then $ax = (a-y)b$, whence, since $(a, b) = 1$, $b \mid x$, whence $x \geqslant b$ and then $ab = ax+by \geqslant ab+by > ab$, which is impossible.

COROLLARY 3. *Given natural numbers $a > 1, m, n$. Then*

$$(a^m-1, a^n-1) = a^{(m,n)}-1\,.$$

PROOF. Let $\delta = (m, n)$. Then $m = \delta m_1$, $n = \delta n_1$, where m_1 and n_1 are relatively prime natural numbers. In virtue of Theorem 16 there exist natural numbers u, v such that $m_1 u-n_1 v = 1$, hence $\delta = mu-nv$. Let $d = (a^m-1, a^n-1)$. Clearly, $a^{(m,n)}-1 \mid a^m-1$ and $a^{(m,n)}-1 \mid a^n-1$, which implies that $a^{(m,n)}-1 \mid d$. On the other hand, we have $d \mid a^m-1$, whence $d \mid a^{mu}-1$ and $d \mid a^n-1$, and this implies $d \mid a^{nv}-1$. Hence $d \mid a^{mu}$ $-a^{nv} = a^{nv}(a^{mu-nv}-1) = a^{nv}(a^{\delta}-1)$. Since $d \mid a^m-1$ and $a > 1$, we have $(d, a) = 1$ and hence $d \mid a^{\delta}-1$, consequently $d \mid a^{(m,n)}-1$, which, by the formula $a^{(m,n)}-1 \mid d$, gives $a^{(m,n)}-1 = d = (a^m-1, a^n-1)$, as required. ☐

So far we have proved that for a linear equation of the type (19) the integral solutions are given by formulae (23). Now we are going to consider the general case of linear equation (18) with arbitrarily many variables m. The following proof of the fact that there is a method for finding the solution of equation (18) seems the simplest and easiest to remember.

We note first that we may confine ourselves to considering only equations (18) where a_i's, $i = 1, 2, \ldots, m$, are natural numbers. This is because coefficients equal to zero do not affect the solutions and if any of the a_i's is negative we may replace it by $-a_i$ and change the sign at the variable.

If any two of the coefficients a_i, $i = 1, 2, \ldots, m$ are equal, for instance $a_1 = a_2$, then setting $x_1 + x_2 = x$ we obtain the equation

$$a_1 x + a_3 x_3 + a_4 x_4 + \ldots + a_m x_m = b. \tag{24}$$

From every integral solution $x_1, x_2, \ldots, x_m$ of equation (18) we can derive a solution $x, x_3, x_4, \ldots, x_m$ of equation (24) putting $x = x_1 + x_2$. Conversely, from every integral solution $x, x_3, x_4, \ldots$ of (24) we can derive a solution of (18) letting x_1 be an arbitrary integer, $x_2 = x - x_1$. Thus, the problem of finding all integral solutions of equation (18) in the case where two of its coefficients are equal is equivalent to the analogous problem for equation (24) in which less number of variables occurs. If any two coefficients of equation (24) are equal we can proceed in the same way, decreasing further the number of variables. Thus, we may suppose that the coefficients of equation (18) are all different natural numbers. Let, a_1 say, be the greatest of them. Then, in particular $a_1 > a_2$. Suppose that the division of a_1 by a_2 yields the quotient k and the remainder a'_2. We then have $a_1 = a_2 k + a'_2$, where k is a natural number and a'_2 is an integer such that $0 < a'_2 < a_2$. Set $x'_1 = kx_1 + x_2$, $x'_2 = x_1$, $a'_1 = a_2$. We have $a_1 x_1 + a_2 x_2 = a_2(kx_1 + x_2) + a'_2 x_1 = a'_1 x'_1 + a'_2 x'_2$. Thus equation (24) can be written in the form

$$a'_1 x'_1 + a'_2 x'_2 + a_3 x_3 + \ldots + a_m x_m = b. \tag{25}$$

From every integral solution $x_1, x_2, \ldots, x_m$ of equation (24) we derive an integral solution $x'_1, x'_2, x_3, \ldots, x_m$ of equation (25) putting $x'_1 = kx_1 + x_2, x'_2 = x_1$. Conversely, from every integral solution $x'_1, x'_2, x_3, \ldots, x_m$ of equation (25) we derive an integral solution of (18) putting $x_1 = x'_2, x_2 = x'_1 - kx'_2$.

Thus the problem of finding the integral solutions of equation (18) reduces to that of solving equation (25) in which the greatest of the coefficients at the variables is less than the corresponding one in equation (18). Continuing, from equation (25) we can similarly obtain an equation in which the greatest of the coefficients at the variables is less than the corresponding one in (25). This process leads to an equation in one variable, which, if solvable, of course, can be easily solved.

Thus we have proved that for a linear equation with integral coefficients there exists a method for finding all the integral solutions. The method we have presented here is far from being the most convenient rule for finding integral solution of a linear equation in practice, it is just simple enough to present it as a proof of the existence of the solutions. The question of finding the method which is most convenient in practice is not of our interest now.

It is worth-while to note that if in (18) one of the coefficients $a_1, a_2, \dots, a_m$, for instance a_1, equals 1, then all the integral solutions of (18) are simply obtained by taking arbitrary integers for $x_2, x_3, \dots, x_m$ and putting

$$x_1 = b - a_2 x_2 - a_3 x_3 - \dots - a_m x_m .$$

It is easy to see that if equation (18) is solvable in integers and $m > 1$, then it necessarily has infinitely many integral solutions. In fact, if $y_1, y_2, \dots, y_m$ are integers such that $a_1 y_1 + a_2 y_2 + \dots + a_m y_m = b$, then putting $x_i = y_i + a_m t_i$ for $i = 1, 2, \dots, m-1$ and $x_m = y_m - a_1 t_1 - \dots - a_{m-1} t_{m-1}$, where $t_1, t_2, \dots, t_{m-1}$ are arbitrary integers, we obtain integers $x_1, x_2, \dots, x_m$ satisfying equation (18).

It is also easy to prove that if equation (18) has an integral solution $x_1, x_2, \dots, x_m$ then the integers $x_1, x_2, \dots, x_m$ can be written as linear combinations of $m-1$ integral parameters.

This property enables us to find the integral solutions of the systems of n linear equations of m variables. In order to do this we express each of the variables of the first equations as a linear combination with integral coefficients of $m-1$ parameters and substitute them for the variables in the remaining $n-1$ equations. Thus, regarding the parameters as variables we obtain a system of $n-1$ equations of $m-1$ variables. Proceeding in this way we finally arrive either at one equation (of one or more variables), which we have already learned how to solve, or to one or more equations with one variable.

12. Chinese Remainder Theorem

THEOREM 17. *Suppose that m is a natural number $\geqslant 2$, $a_1, a_2, \dots, a_m$ are natural numbers such that any two of them are relatively prime, and $r_1, r_2, \dots, r_m$ are arbitrary integers. Then there exist integers $x_1, x_2, \dots, x_m$ such that*

$$a_1 x_1 + r_1 = a_2 x_2 + r_2 = \dots = a_m x_m + r_m . \tag{26}$$

PROOF. The theorem is true for $m = 2$, since if a_1, a_2 are relatively prime, the equation $a_1 x - a_2 y = r_2 - r_1$ has an integral solution in x and y.

Now let m be an arbitrary natural number $\geqslant 2$. Suppose that Theorem 17 is true for the number m. Let $a_1, a_2, \dots, a_m, a_{m+1}$ be natural numbers such that any two of them are relatively prime and let $r_1, r_2, \ldots, r_m, r_{m+1}$ be arbitrary integers. From the assumption that the theorem is true for the number m we infer that there exist integers $x_1, x_2, \ldots, x_m$ satisfying equation (26). Since each of the numbers $a_1, a_2, \ldots, a_m$ is relatively prime to the number a_{m+1}, then, by Theorem 6^a, the number $a_1 a_2 \ldots a_m$ is also relatively prime to a_{m+1} and therefore, as we know, there exist integers t and u such that

$$a_1 a_2 \ldots a_m t - a_{m+1} u = r_{m+1} - a_1 x_1 - r_1 .$$

We set

$$x_i' = \frac{a_1 a_2 \ldots a_m}{a_i} t + x_i, \qquad \text{where} \qquad i = 1, 2, \ldots, m \text{ and } x_{m+1}' = u .$$

Plainly the numbers $x_1', x_2', \ldots, x_{m+1}'$ are integers and, as is easy to check,

$$a_1 x_1' + r_1 = a_2 x_2' + r_2 = \ldots = a_{m+1} x_{m+1}' + r_{m+1} ,$$

which by induction, completes the proof of the theorem. □

It follows from Theorem 17 that if any two of $m \geqslant 2$ natural numbers $a_1, a_2, \ldots, a_m$ are relatively prime and $r_1, r_2, \ldots, r_m$ are arbitrary integers, then there exists an integer k such that dividing k by $a_1, a_2, \ldots, a_m$ we obtain the remainders $r_1, r_2, \ldots, r_m$, respectively. This, by the way, is the reason why the theorem is called the remainder theorem.

It is obvious that adding to k an arbitrary multiple of the number $a_1 a_2 \ldots a_m$, we obtain an integer which divided by $a_1, a_2, \ldots, a_m$ gives also the remainders $r_1, r_2, \ldots, r_m$, respectively. It follows that there exist infinitely many integers which have this property.

We present here a simple application of Theorem 17. Let m and s be two given natural numbers. We proved in § 4 that any two different terms of the sequence $F_k = 2^{2^k} + 1$ $(k = 0, 1, 2, \ldots)$ are relatively prime. Put $a_i = F_i^s$ and $r_i = -i$ for all $i = 1, 2, \ldots, m$. For $c = a_1 x_1 + r_1$ formulae (26) imply that $F_i^s x_i = a_i x_i = a_1 x_1 + r_1 - r_i = c + i$, whence $F_i^s \mid c + i$ for all $i = 1, 2, \ldots, m$. Since $F_i > 1$ for $i = 1, 2, \ldots$, each of the numbers $c+1$, $c+2, \ldots, c+m$ is divisible by the s-th power of a natural number greater than 1. Thus we have proved the following assertion:

For each natural number s there exist arbitrarily long sequences of consecutive natural numbers, each of them divisible by the s-th power of a natural number greater than 1.

13. Thue's Theorem

THEOREM 18 (Thue [1]). *If m is a natural number and a an integer relatively prime to m, then there exist natural numbers x and y both less than $\sqrt{m}$ and such that the number $ax \pm y$ is divisible by m for a suitable choice of the ambiguous sign $\pm$.*

PROOF. The theorem is, of course, true for $m = 1$, since in this case we may set $x = y = 1$. Suppose that m is a natural number greater than 1. Let q denote the greatest natural number less than or equal to $\sqrt{m}$. Then, clearly, $q+1 > \sqrt{m}$ and hence $(q+1)^2 > m$. Consider the expressions $ax-y$, for x, y taking the values $0, 1, 2, \ldots, q$. There are $(q+1)^2 > m$ of them and, since there are only m different remainders obtained from division by m, for two different pairs x_1, y_1 and x_2, y_2, where, for instance, $x_1 \geqslant x_2$, one obtains the same remainders from division of $ax-y$ by m. Consequently the number $ax_1 - y_1 - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$ is divisible by m. We cannot have $x_1 = x_2$, since then the number $y_1 - y_2$ would be divisible by m, which, in view of the fact that $0 \leqslant y_1 \leqslant q \leqslant \sqrt{m} < m$ (since $m > 1$) and similarly $0 \leqslant y_2 < m$, is impossible because the pairs x_1, y_1 and x_2, y_2 were different. The equality $y_1 = y_2$ is also impossible, since then the number $a(x_1 - x_2)$ would be divisible by m, which, in view of the fact that the number a is relatively prime to m, would imply that $m \mid (x_1 - x_2)$, and this, in virtue of the inequalities $0 \leqslant x_1 \leqslant q < m$, $0 \leqslant x_2 \leqslant q$ and $x_1 \neq x_2$, is impossible. Thus we have both $x_1 \neq x_2$ and $y_1 \neq y_2$. Since $x_1 \geqslant x_2$, $x = x_1 - x_2$ is a natural number. The number $y_1 - y_2$ can be a negative integer, but certainly it is different from zero, so $y = |y_1 - y_2|$ is a natural number. We see that $x = x_1 - x_2 \leqslant x_1 \leqslant q \leqslant \sqrt{m}$, $y \leqslant q \leqslant \sqrt{m}$ and that for the appropriate sign $+$ or $-$ the number $a(x_1 - x_2) - (y_1 - y_2) = ax \pm y$ is divisible by m, and this is what the Thue theorem states. □

By a slight modification of the proof given above we could have the following generalization of the theorem Scholz and Schoenberg proved ([1], p. 44):

If m, e and f are natural numbers such that $e \leqslant m$, $f \leqslant m < ef$, then for each integer a with $(a, m) = 1$ there exist integers x and y such that for the appropriate sign $+$ or $-$ we have

$$m \mid ax \pm y \quad \textit{and} \quad 0 \leqslant x \leqslant f, \quad 0 \leqslant y \leqslant e.$$

For other generalizations of the Thue theorem, see Brauer and Reynolds [1], Mordell [6] and Nagell [6].

14. Square-free numbers

An integer is called *square-free* if it is not divisible by the square of any natural number > 1. The square-free natural numbers $\leqslant 20$ are the following: 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19.

It follows from the assertion proved at the end of § 12 that there exist arbitrarily long sequences of consecutive natural numbers such that none of them is square-free. Among every four consecutive natural numbers at least one is not square-free (since at least one of them is divisible by $4 = 2^2$). One can prove that there exist infinitely many triples of consecutive natural numbers such that each of the numbers is square-free.

It can be proved that each natural number > 1 is the sum of two square-free natural numbers and in infinitely many ways a difference of such numbers (Nagell [1], cf. Sierpiński [36]). It is also true that each sufficiently large natural number is the sum of the square-free number and the square of a natural number (Esterman [1]; cf. Hooley [1]).

We prove

THEOREM 19. *Each natural number n can be uniquely represented in the form $n = k^2l$, where k and l are natural numbers and l is square-free.*

PROOF. For a given natural number n, let k denote the greatest natural number such that $k^2 \mid n$. We have $n = k^2l$, where l is a natural number. If l were not square-free, then we would have $l = r^2s$, where r, s are natural numbers and $r > 1$. Thus $n = (kr)^2s$ and consequently $(kr)^2 \mid n$, where $kr > k$, contrary to the definition of k.

Now suppose that $n = k_1^2 l_1$, where k_1, l_1 are natural numbers and l_1 is square-free. Let $d = (k, k_1)$. We have $k = dh$, $k_1 = dh_1$, where h, h_1 are natural numbers and $(h, h_1) = 1$. Since $n = d^2h^2l = d^2h_1^2 l_1$, we have $h^2l = h_1^2 l_1$ and, since $(h^2, h_1^2) = 1$, by Theorem 5, we obtain $h^2 \mid l_1$, which proves that $h = 1$, since l_1 is square-free. This implies that $k = dh = d$. But since $d \mid k_1$, we have $k \mid k_1$, whence $k \leqslant k_1$ which, in virtue of the definition of k and the equality $n = k_1^2 l_1$, implies $k = k_1$, whence also $l = l_1$. □

CHAPTER II

DIOPHANTINE ANALYSIS OF SECOND AND HIGHER DEGREES

1. Diophantine equations of arbitrary degree and one unknown

The name of Diophantine analysis bears a branch of the theory of numbers concerning equations which are to be solved in integers. The equations themselves are called *Diophantine.* They are named after a Greek mathematician Diophantus who lived in Alexandria in the third century A. D. and occupied himself with problems reducible to the equations of the above-mentioned type.

We start with the equations of arbitrary degree and one unknown.

Suppose that the left-hand side of an equation is a polynomial with integral coefficients, i.e. let the equation be of the form

$$(1)\qquad a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0,$$

where m is a given natural number and $a_0, a_1, \ldots, a_m$ are integers with $a_0 \neq 0$ and $a_m \neq 0$.

If there is an integer x satisfying equation (1), then

$$(a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-1}) x = -a_m.$$

It follows that the integer x must be a divisor of the integer a_m, therefore, since the integer a_m, being different from zero, has finitely many divisors, all the integral solutions of equation (1) can be found in finitely many trials. We just substitute the divisors (positive and negative as well) of a_m successively in equation (1) and select those which satisfy the equation. If $a_m = 0$, then clearly $x = 0$ is a solution of the equation. The other solutions are obtained by considering the equation

$$a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-2} x + a_{m-1} = 0,$$

whose solutions are found in analogy to the previous case whenever $a_{m-1} \neq 0$. If $a_{m-1} = 0$, then the equation turns into an equation of degree $m-2$ and we repeat the same reasoning.

As an example we consider the equation

$$x^7 + x + 2 = 0.$$

As follows from the above, the solutions of the equation are to be found among the divisors of the integer -2, and these are $1, -1, 2, -2$. We see that only the number -1 satisfies the equation; thus it is the only integral solution of our equation.

The reasoning just presented shows that there are no real difficulties, apart from the technical ones, in finding all the integral roots of a polynomial with integral coefficients, even when the polynomial is of a higher degree. This situation is quite different from what appears in algebra, where, as we know, the formulae for the roots of polynomials of the third and fourth degree are very complicated and for some polynomials of degree higher than four the roots cannot be found by algebraic methods at all.

Similarly, the task of finding all the rational roots of polynomial with integral coefficients does not involve any real difficulty. As a matter of fact, suppose that a rational number r satisfies equation (1) with integral coefficients $a_0, a_1, \ldots, a_m$. We may suppose that $a_0 \neq 0$, and moreover, excluding the possible root $r = 0$, that $a_m \neq 0$. The number r can be represented in the form of $r = k/s$, where s is a natural number, k an integer and $(k, s) = 1$.

From equation (1), for $x = k/s$, we obtain

$$a_0 k^m = -(a_1 k^{m-1} + a_2 k^{m-2} s + \ldots + a_m s^{m-1}) s,$$

$$a_m s^m = -(a_0 k^{m-1} + a_1 k^{m-2} s + \ldots + a_{m-1} s^{m-1}) k.$$

The first of these equalities proves that $s \mid a_0 k^m$, which, since $(k, s) = 1$, implies $s \mid a_0$. The second shows that $k \mid a_m s^m$, whence, in virtue of $(k, s) = 1$, we obtain $k \mid a_m$. Thus the rational solutions of the equation can be found in finitely many trials: we substitute for x irreducible fractions $\frac{k}{s}$, where the k's are divisors of the integer a_m and the s's are natural divisors of the integer a_0, and select those which satisfy the equation.

2. Problems concerning Diophantine equations of two or more unknowns

We present here some questions which can be asked about the integral solutions of an equation of two or more unknowns.

We list them in order of increasing difficulty:

Given an equation of two or more unknowns:

1. Does it have at least one integral solution?
2. Is the number of its integral solutions finite or infinite?
3. Find all its integral solutions.

There are equations for which the answer to none of these questions is known. We do not know, for instance, whether the equation $x^3+y^3+z^3 = 30$ has any integral solution at all. We know four integral solutions of equation $x^3+y^3+z^3 = 3$, namely $(x, y, z) = (1, 1, 1)$, $(4, 4, -5)$, $(4, -5, 4)$, $(-5, 4, 4)$, but we do not know whether they are all the integral solutions of this equation. (There are no others with $|x+y+z| \leqslant 150\,000$, see Scarowsky and Boyarsky [1]). The difficulty of this problem was compared by L. J. Mordell [5] with the difficulty of deciding whether the sequence 1, 2,..., 9 appears in decimal expansion of π.

It is known that the equation $x^3+y^3+z^3 = 2$ has infinitely many solutions in integers, e.g. $(x, y, z) = (1+6n^3, 1-6n^3, -6n^2)$, where n is an arbitrary natural number. We do not know, however, all the integral solutions of this equation.

On the other hand, one can prove that the equation $x^3+y^3+z^3 = 4$ has no integral solutions. In fact, the only possible values for the remainder obtained by dividing the cube of an integer by 9 are 0, 1, and 8. Hence the only possible values for the remainder obtained by dividing the sum of the cubes of two integers by 9 are 0, 1, 2, 7, 8, and similarly dividing the sum of the cubes of three integers we obtain as the only possible values for the remainder the integers 0, 1, 2, 3, 6, 7, 8 but neither 4 nor 5. Thus not only the equation $x^3+y^3+z^3 = 4$ but also the equation $x^3+y^3+z^3 = 5$ has no integral solutions x, y, z (more generally, the equation $x^3+y^3+z^3 = k$, where k divided by 9 gives the remainder 4 or 5, has no integral solutions).

We know that the equation $x^3+y^3+z^3 = 6$ has integral solutions x, y, z, for instance $(x, y, z) = (-1, -1, 2), (-43, -58, 65), (-55, -235, 236)$, but we do not know whether the number of the solutions in integers is finite.

Sometimes the difficulties of finding all the integral solutions of an equation are purely of technical nature; i.e. we know the method for finding the solutions but the calculations it involves are too long to be carried out; for instance, such is the case with finding the solutions of the equation $xy = 2^{293}-1$ in integers. One can prove that it has a solution in x and y, each greater than 1 (¹), but we cannot find it. Clearly, there exists a method for finding that solution: namely we may divide the number $2^{293}-1$ by numbers less than $2^{293}-1$, successively, and select those

---

(¹) See Chapter X. § 3.

numbers for which the remainder is zero. The calculations it involves, however, are much too long for the present technical means.

On the other hand, we do not know any method permitting us, even after long calculations, to decide whether the equation $x^3+y^3+z^3 = 30$ is or is not solvable in integers. It is easy to prove, however, that the equation has no solution in positive integers; the proof of this we leave to the reader.

3. The equation $x^2+y^2 = z^2$

We are going to consider a particular equation of the second degree with three unknowns,

$$x^2+y^2 = z^2, \tag{2}$$

called the *Pythagorean equation.*

As is known, this equation is particularly important in trigonometry and analytic geometry, and a special case of it, for $x = y$, is connected with the simplest proof of the existence of irrational numbers.

We are going to find all the integral solutions of equation (2). We exclude the obvious solutions, in which one of the numbers x, y is zero. Among the remaining ones we may consider only those which are natural numbers, since the change of the sign at an unknown does not affect the equation. If the numbers x, y, z are natural and satisfy equation (2), then we say that (x, y, z) is a *Pythagorean triangle.* I have devoted to such triangles a special book, cf. Sierpiński [35].

A solution of equation (2) is called a *primitive solution* if the numbers x, y, z are natural and have no common divisor greater than one.

If ξ, η, ζ is a primitive solution of (2), and d an arbitrary natural number, then

$$x = d\xi, \qquad y = d\eta, \qquad z = d\zeta \tag{3}$$

is also a solution of equation (2). In fact, if $\xi^2+\eta^2 = \zeta^2$, then multiplying both sides by d^2 and using (3) we obtain equation (2).

Conversely, if x, y, z is a solution of equation (2) in natural numbers, then, putting $(x, y, z) = d$ we have $x = d\xi$, $y = d\eta$, $z = d\zeta$, where $(\xi, \eta, \zeta) = 1$ (cf. Chapter I, theorem 3^a). Then, in virtue of (2) we have $(d\xi)^2+(d\eta)^2 = (d\zeta)^2$. Dividing this equation throughout by d^2 we see that the natural numbers ξ, η, ζ constitute a primitive solution of equation (2).

We say that a solution of equation (2) in natural numbers x, y, z belongs to the dth class if $(x, y, z) = d$.

In virtue of what we have stated above, in order to obtain all the solutions in natural numbers belonging to the dth class, it suffices to multiply all the primitive solutions of equation (2) by d. Thus, without loss of generality, we may confine ourselves to finding only the primitive solutions of equation (2).

Suppose that x, y, z is a primitive solution of equation (2). We prove that one of the numbers x, y is even and the other is odd. Suppose that this is not the case, i.e. that both of them are either even or odd. In the first case the number $x^2+y^2 = z^2$ would be even, and thus also the number z would be even, and hence the numbers x, y, z would have a common divisor 2, contrary to the assumption. In order to show that the second case is also impossible we prove that

Dividing the square of an odd natural number by 8 *we obtain the remainder* 1.

In order to see this we note that an odd number can be written in the form $2k-1$, where k is an integer. Hence $(2k-1)^2 = 4k^2-4k+1 = 4k(k-1)+1$. But one of the numbers k and $k-1$ must be even; thus it is divisible by 2, whence the number $4k(k-1)$ is divisible by 8, and thus dividing $(2k-1)^2$ by 8 we obtain the remainder 1, as required.

Consequently, dividing the sum of the squares of two natural numbers by 8 we obtain the remainder 2, which, in virtue of what we proved above, shows that the sum of the squares of two odd natural numbers is not the square of an odd number. It cannot be the square of an even number, either, since in this case it would be divisible by 4, and so the remainder obtained by dividing it by 8 would be 0 or 4.

Thus we have proved that formula (2) cannot hold for x, y being odd and z being an integer. It follows that if x, y, z is a primitive solution of equation (2), then one of the numbers x, y, say y, is even, and the other one, x, is odd. The remaining solutions are simply obtained by interchanging x and y.

If in a given solution of equation (2), the number y is even and the number x is odd, then the number z is odd. Equation (2) can be written in the form

$$y^2 = (z+x)(z-x). \tag{4}$$

The numbers $z+x$ and $z-x$, as the sum and the difference of two odd numbers respectively, are both even. Consequently,

$$z+x = 2a, \qquad z-x = 2b, \tag{5}$$

where a and b are natural numbers. Hence

$$z = a+b, \qquad x = a-b.$$

These equalities imply that the numbers a and b must be relatively prime, since otherwise they would have a common divisor $\delta > 1$, and then we would have $z = k\delta$, $x = l\delta$, where k and l would be natural numbers. Hence $y^2 = z^2-x^2 = (k^2-l^2)\delta^2$, whence the number y^2 would be divisible by δ^2 and consequently, y by δ (cf. Chapter I, § 6, Corollary 2), which is impossible, since x, y, z is a primitive solution; therefore $\delta > 1$ cannot divide all the numbers x, y, z.

By assumption, the number y is even, consequently $y = 2c$, where c is a natural number. In virtue of (5), equation (4) implies the equality $4c^2 = 4ab$, whence

$$c^2 = ab. \tag{6}$$

But since $(a, b) = 1$, in virtue of Theorem 8 of Chapter I, equality (6) implies that each of the numbers a, b is a square. That is $a = m^2$, $b = n^2$, where m, n are natural numbers and $(m, n) = 1$ (since $(a, b) = 1$). Hence

$$z = a+b = m^2+n^2, \qquad x = a-b = m^2-n^2,$$

and, since $c^2 = ab = m^2 n^2$ and $y = 2c$,

$$y = 2mn.$$

We have thus proved that if x, y, z is a primitive solution of equation (2) and y is an even number, then

$$x = m^2-n^2, \qquad y = 2mn, \qquad z = m^2+n^2, \tag{7}$$

where m, n are natural numbers, $(m, n) = 1$ and of course, $m > n$, because x is a natural number. Moreover, one of the numbers m, n is even, the other is odd. In fact, they cannot both be even, since they are relatively prime. They cannot both be odd either, since, if they were, then, in virtue of (7) all the numbers x, y, z would be even, which is impossible, since $(x, y, z) = 1$. Thus $2\,|\,mn$, which implies that the number $y = 2mn$ is divisible by 4.

We prove that converse is also true: if m, n are two relatively prime natural numbers, $m > n$, and one of them odd and the other even, then the numbers x, y, z obtained from m, n by formulae (7) constitute a primitive solution of equation (2).

To do this we note first that the numbers x, y, z obtained from formulae (7), m, n being natural and $m > n$, constitute a solution of equation (2). We simply check that

$$(m^2-n^2)^2+(2mn)^2 = (m^2+n^2)^2. \tag{8}$$

Now, using the fact that the numbers m, n are relatively prime, we prove that $(x, y, z) = 1$. If this were not the case, then there would exist a common divisor $\delta > 1$ of the numbers x, y, z. The number δ could not be even, since the number $z = m^2+n^2$, as the sum of an odd and an even number is odd. But in virtue of (7),

$$2m^2 = x+z, \qquad 2n^2 = z-x; \tag{9}$$

therefore the numbers m^2 and n^2 would both be divisible by δ, which is clearly false, since the equality $(m, n) = 1$ implies $(m^2, n^2) = 1$.

Formulae (9) prove that to different numbers m, n there correspond different solutions x, y, z.

The results we have just obtained can be formulated in the following

THEOREM 1. *All the primitive solutions of the equation $x^2+y^2 = z^2$ for which y is an even number are given by the formulae*

$$x = m^2-n^2, \qquad y = 2mn, \qquad z = m^2+n^2, \tag{10}$$

where m, n are taken to be pairs of relatively prime natural numbers, one of them even and the other odd and m greater than n.

As has been noticed by J. Ginsburg [1], in order to find, for a given primitive solution of the equation $x^2+y^2 = z^2$, the numbers m, n satisfying the conditions of Theorem 1 (sometimes called the *generators* of the solution) it is, of course, sufficient to present the rational number $(x+z)/y$ in the form of the irreducible fraction m/n.

In order to list systematically all the primitive solutions of equation (2) we take values 2, 3, 4, ... for the number m successively and then for each of them we take those numbers n which are relatively prime to m, less than m and being even whenever m is odd.

Here is the table of the first twenty primitive solutions listed according to the above-mentioned rule.

m	n	x	y	z	area	m	n	x	y	z	area
2	1	3	4	5	6	7	6	13	84	85	546
3	2	5	12	13	30	8	1	63	16	65	504
4	1	15	8	17	60	8	3	55	48	73	1320
4	3	7	24	25	84	8	5	39	80	89	1560
5	2	21	20	29	210	8	7	15	112	113	840
5	4	9	40	41	180	9	2	77	36	85	1386
6	1	35	12	37	210	9	4	65	72	97	2340
6	5	11	60	61	330	9	8	17	144	145	1224
7	2	45	28	53	630	10	1	99	20	101	990
7	4	33	56	65	924	10	3	91	60	109	2730

As we know, in order to obtain all the solutions in natural numbers of equation (2) one has to multiply each of the primitive solutions by natural numbers 1, 2, 3, ... succesively, and then add the solutions obtained from the previous ones by interchanging x and y. Moreover, every solution in natural numbers of equation (2) is obtained in this way precisely once.

As follows from identity (8), substituting natural numbers m, n with $m > n$ in formulae (7) we obtain solutions in natural numbers of equation (2). But even adding all the solutions obtained in this way with the numbers x and y interchanged we do not get all the solutions in natural numbers of equation (2). E.g. we do not obtain from (7) the solution 9, 12, 15, since there are no natural numbers m and $n < m$ for which $15 = m^2+n^2$; for, none of the numbers $15-1^2 = 14$, $15-2^2 = 11$, $15-3^2 = 6$ is the square of a natural number.

All the solutions of equation (2) are given by the following formulae

$$x = (m^2-n^2)\,l, \qquad y = 2mnl, \qquad z = (m^2+n^2)\,l,$$

where m, $n < m$ and l are natural, provided the solutions with numbers x and y interchanged are added to them. The above-mentioned formulae, however, give the same solution for different systems of the natural numbers m, n, l; for instance, the solution 12, 16, 20 is obtained for $m = 2$, $n = 1$, $l = 4$ as well as for $m = 4$, $n = 2$, $l = 1$, and the solution 48, 64, 80 is obtained for $m = 8$, $n = 4$, $l = 1$, as well as for $m = 4$, $n = 2$, $l = 4$ and for $m = 2$, $n = 1$, $l = 16$.

The first of the solutions listed in the table presented above is the solution of equation (2) with x, y, z being the least possible natural numbers. Moreover, in this solution the numbers x, y, z are consecutive natural numbers. It is not difficult to prove that this is the unique solution of equation (2) consisting of consecutive natural numbers. In fact, if three consecutive natural numbers $n-1$, n, $n+1$ satisfy the equation $(n-1)^2+n^2 = (n+1)^2$, then $n^2 = 4n$, whence, dividing both sides by n, we obtain $n = 4$, i.e. the solution 3, 4, 5.

It is easy to prove that the equation $3^n+4^n = 5^n$ has no solutions in natural numbers n except one, $n = 2$.

For, we have $3+4 > 5$, whence $n = 1$ cannot be a solution of the equation. Further, we have $3^2+4^2 = 5^2$, whence, for $n > 2$, $5^n = 5^2\cdot 5^{n-2} = 3^2\cdot 5^{n-2}+4^2\cdot 5^{n-2} > 3^2\cdot 3^{n-2}+4^2\cdot 4^{n-2} = 3^n+4^n$. Therefore $3^n+4^n \neq 5^n$ for $n > 2$.

It would be not difficult to prove a more general statement, namely that if $a^2+b^2 = c^2$, then $a^n+b^n < c^n$ for all $n > 2$.

It is also true that the equation $3^x+4^y = 5^z$ has no solutions in natural numbers x, y, z except one, $x = y = z = 2$, but this is not so easy to prove (Sierpiński [17], cf. Nagell [11]).

L. Jeśmanowicz [1] has proved that the only solution of each of the equations

$$5^x+12^y = 13^z, \quad 7^x+24^y = 25^z, \quad 9^x+40^y = 41^z, \quad 11^x+60^y = 61^z$$

in natural numbers x, y, z is $x = y = z = 2$. He asks whether there exist natural numbers a, b, c such that $a^2+b^2 = c^2$ for which the equation $a^x+b^y = c^z$ has a solution in natural numbers x, y, z different from $x = y = z = 2$ (cf. Ko Chao [2], [3], [4]).

It is known that there exist infinitely many Pythagorean primitive triples (a, b, c), such that the equation $a^x+b^y = c^z$ has no solutions in natural numbers x, y, z except one: $x = y = z = 2$ (Lu Wen-Twan [1], Józefiak [2], Podsypanin [1], Dem'yanenko [1]).

It has been proved above that for each primitive solution of equation (2) one of the numbers x, y which is even is divisible by 4. Thus, a fortiori, *in every solution of equation* (2) *in integers* x, y, z *at least one of the numbers* x, y *is divisible by* 4.

We prove that *in every solution of equation* (2) *in integers at least one of the numbers* x, y *is divisible by* 3.

In the contrary case, we would have $x = 3k\pm 1$, $y = 3l\pm 1$, k and l being integers. Hence $x^2+y^2 = 3(3k^2+3l^2\pm 2k\pm 2l)+2$. But this cannot possibly be the square of a natural number, since the square of a number divisible by 3 is divisible by 3, and the square of an integer which is not divisible by 3, that is a number of the form $(3t\pm 1)^2 = 3(3t^2\pm 2t)+1$, divided by 3 yields the remainder 1.

Now we are going to prove that *in every integer solution of equation* (2) *at least one of the numbers* x, y, z *is divisible by* 5.

To prove this we consider first an arbitrary integer m which is not divisible by 5. We have $m = 5k\pm 1$ or $m = 5k\pm 2$, where k is an integer. In the first case $m^2 = 5(5k^2\pm 2k)+1$, in the second $m^2 = 5(5k^2\pm 4k)+4$. Consequently, dividing by 5 the square of an integer not divisible by 5 we obtain the remainder equal to 1 or 4. Thus applying the above remark to the numbers x, y, z, we see that if none of the numbers x, y, z were divisible by 5, then each of the numbers x^2 and y^2 divided by 5 would yield the remainder 1 or 4, whence the number x^2+y^2 divided by 5 would produce the remainder 2, 3, or 0. Since $x^2+y^2 = z^2$, the first two cases are, clearly, impossible; for, dividing the number z^2 by 5, we cannot obtain the remainder 2 or 3. Hence, the third possibility must occur, and this proves that the number z^2, and hence the number z, is divisible by 5. Thus we conclude that if neither of the numbers x, y, is divisible by 5, then the number z is divisible by 5.

Since (3, 4, 5) is a Pythagorean triangle, we see that the numbers 1, 2, 3, 4, 5 are the only natural numbers n for which the assertion that in every Pythagorean triangle at least one of the sides of the triangle is divisible by n is true.

Now we are going to consider the solutions of equation (2) for which two of the numbers x, y, z are consecutive natural numbers. Clearly, the solutions belonging to this class are primitive. Therefore z is an odd number, and so $z-y = 1$ can hold only if y is even.

Consequently, by (10), $m^2+n^2-2mn = z-y = 1$, or equivalently, $(m-n)^2 = 1$ which, since $m > n$, implies that $m-n = 1$, i.e. $m = n+1$. Hence $x = m^2-n^2 = (n+1)^2-n^2 = 2n+1$, $y = 2n(n+1)$, $z = y+1 = 2n(n+1)+1$.

Thus all the solutions of equation (2) in natural numbers x, y, z with $z-y = 1$ are given by the formulae

$$x = 2n+1, \qquad y = 2n(n+1), \qquad z = 2n(n+1)+1$$
$$\text{for} \quad n = 1, 2, 3, \ldots$$

We list the first 10 solutions of this kind:

n	x	y	z
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41
5	11	60	61

n	x	y	z
6	13	84	85
7	15	112	113
8	17	144	146
9	19	180	181
10	21	220	221

And here are some other solutions of this kind:

n	x	y	z
10	21	220	221
100	201	20200	20201
1000	2001	2002000	2002001

n	x	y	z
20	41	840	8004001
200	401	80400	80401
2000	4001	8004000	8004001

and so on (Willey [1]).

The next section is devoted to the solutions for which $x-y = \pm 1$.

4. Integral solutions of the equation $x^2+y^2 = z^2$ for which $x-y = \pm 1$

Among the primitive solutions of equation (2) listed in § 3 we see two solutions of the kind defined in the title of this section, namely: 3, 4, 5 and 21, 20, 29. It is easy to prove that there are infinitely many such solutions. This follows immediately from the fact that if for natural numbers x and z the equality $x^2+(x+1)^2 = z^2$ holds, then

$$(3x+2z+1)^2+(3x+2z+2)^2 = (4x+3z+2)^2.$$

In fact, $(3x+2z+1)^2+(3x+2z+2)^2 = 18x^2+24xz+8z^2+18x+12z+5$, but since $x^2+(x+1)^2 = z^2$, we have $2x^2+2x+1 = z^2$, whence

$$\begin{aligned}(3x+2z+1)^2+(3x+2z+2)^2 &= 16x^2+24xz+9z^2+16x+12z+4\\ &= (4x+3z+2)^2.\end{aligned}$$

Thus from a given Pythagorean triangle whose catheti are consecutive natural numbers we obtain another Pythagorean triangle with the same property. Starting with the triangle 3, 4, 5 we obtain by this procedure a triangle whose sides are $3\cdot 3+2\cdot 5+1 = 20$, 21 and $4\cdot 3+3\cdot 5+2 = 29$. Similarly, from this triangle we get the triangle whose sides are $3\cdot 20+2\cdot 29+1 = 119$, 120 and $4\cdot 20+3\cdot 29+2 = 169$. We list the first six triangles obtained in this way:

3	4	5
20	21	29
119	120	169
696	697	985
4059	4060	5741
23660	23661	33461

It would not be difficult to prove that this procedure gives triangles with the greater cathetus alternatively even and odd.

Let $x_1 = 3$, $y_1 = 4$, $z_1 = 5$, and for $n = 1, 2, 3 \ldots$ set

$$\begin{gathered}x_{n+1} = 3x_n+2z_n+1, \qquad y_{n+1} = x_{n+1}+1,\\ z_{n+1} = 4x_n+3z_n+2.\end{gathered} \tag{11}$$

We prove that (x_n, y_n, z_n) $(n = 1, 2, \ldots)$ are all the Pythagoran triangles for which the catheti are consecutive natural numbers.

LEMMA. *If natural numbers x, z satisfy the equation*

$$x^2+(x+1)^2 = z^2 \tag{12}$$

and if $x > 3$, *then*

$$x_0 = 3x-2z+1, \qquad z_0 = 3z-4x-2 \tag{13}$$

are natural numbers satisfying the equation

$$x_0^2+(x_0+1)^2 = z_0^2, \tag{14}$$

and $z_0 < z$.

PROOF. In virtue of (13) we have

$$\begin{aligned} x_0^2+(x_0+1)^2 &= 2x_0^2+2x_0+1 = 18x^2+8z^2-24xz+18x-12z+5, \\ z_0^2 &= 16x^2+9z^2-24xz+16x-12z+4. \end{aligned} \tag{15}$$

Since, by (2), $z^2 = 2x^2+2x+1$, we have $16x^2+9z^2-24xz+16x-12z+4 = 8z^2+18x^2-24xz+18x-12z+5$ which, by (15), implies (14).

In view of (13), we see that in order to prove that x_0, z_0 are natural and that $z_0 < z$ one has to show that

$$3x-2z+1 > 0 \quad \text{and} \quad 0 < 3z-4x-2 < z,$$

or, equivalently, that

$$2z < 3x+1, \qquad 3z > 4x+2 \qquad \text{and} \qquad z < 2x+1. \tag{16}$$

Since $x > 3$, we have $x^2 > 3x = 2x+x > 2x+3$, whence, by (12),

$$\begin{gathered} 4z^2 = 8x^2+8x+4 = 9x^2+8x+4-x^2 < \\ < 9x^2+8x+4-(2x+3) = 9x^2+6x+1 = (3x+1)^2, \end{gathered}$$

consequently $2z < 3x+1$ and since $x > 0$, $2z < 4x+1$; therefore $z < 2x+1$. This, by (12) and the fact that $x > 0$, implies

$$9z^2 = 18x^2+18x+9 > 16x^2+16x+4 = (4x+2)^2,$$

whence $3z > 4x+2$, and this completes the proof of formulae (16) and at the same time the proof of the lemma. □

Now suppose that there exist Pythagorean triangles $(x, x+1, z)$ which are different from all the triangles (x_n, x_n+1, z_n) defined above. Among them there exists a triangle (x, y, z) for which z is the least. Then, clearly, x cannot be less than or equal to 3, since if it could, we would have $(x, y, z) = (3, 4, 5)$.

Let

$$u = 3x-2z+1, \qquad v = 3z-4x-2. \tag{17}$$

In virtue of the lemma $(u, u+1, v)$ is a Pythagorean triangle and $v < z$. Thus, since z was the least among all z's of all the Pythagorean triangles different from the triangles (x_n, x_n+1, z_n), for some n we have, $u = x_n$, $v = z_n$ and

$$x_{n+1} = 3u+2v+1, \qquad y_{n+1} = x_{n+1}+1, \qquad z_{n+1} = 4u+3v+2.$$

Hence, by (17),

$$x_{n+1} = 3(3x-2z+1)+2(3z-4x-2)+1 = x,$$
$$z_{n+1} = 4(3x-2z+1)+3(3z-4x-2)+2 = z.$$

So the triangle $(x, x+1, z)$ turns out to be one of the triangles (x_n, y_n, z_n), contrary to the assumption. Thus we have proved that the triangles (x_n, x_n+1, z_n) $(n = 1, 2, ...)$ are all the Pythagorean triangles for which the catheti are consecutive natural numbers.

It can be proved that if the infinite sequences $u_1, u_2, ...$ and $v_1, v_2, ...$ are defined by the conditions $u_0 = 0$, $u_1 = 3$, $u_{n+1} = 6u_n - u_{n-1}+2$ for $n = 1, 2, ...$ and $v_0 = 1$, $v_1 = 5$, $v_{n+1} = 6v_n - v_{n-1}$ for $n = 1, 2, ...$, then $u_n^2 + (u_n+1)^2 = v_n^2$ for $n = 1, 2, ...$, and (u_n, u_n+1, v_n) is the nth triangle of sequence (11).

One can also prove that if $(1+\sqrt{2})^{2n+1} = a_n + b_n\sqrt{2}$ where $n = 1, 2, ...$, a_n and b_n are integers, then $\left(\frac{a_n+(-1)^n}{2}, \frac{a_n-(-1)^n}{2}, b_n\right)$ is the nth triangle of sequence (11).

Now we suppose that the natural numbers x and z satisfy equation (12). Since one of the numbers x, $x+1$ is even and the other is odd, z is odd and, clearly, $z > x+1$ and also $z^2 < (2x+1)^2$. Therefore $u = z-x-1$ and $v = \frac{1}{2}(2x+1-z)$ are natural numbers; thus, in virtue of the identity

$$\frac{(z-x-1)(z-x)}{2} - \left(x+\frac{(1-z)}{2}\right)^2 = \frac{1}{4}(z^2-x^2-(x+1)^2)$$

and the equality $x^2+(x+1)^2 = z^2$, we have

$$\tfrac{1}{2}u(u+1) = v^2. \tag{18}$$

The number $t_u = \frac{1}{2}u(u+1)$, where u is a natural number, is called a *triangular number* (cf. later § 16). Formula (18) shows that the triangular number t_u is the square of a natural number.

Thus every solution of the equation $x^2+(x+1)^2 = z^2$ in natural numbers gives a solution of equation (18) in natural numbers u and v simply by putting $u = z-x-1$, $v = x+(1-z)/2$. The converse is also true: if natural numbers u and v satisfy equation (18), then putting $x = u + 2v$, $z = 2u+2v+1$ and using the identity

$$(u+2v)^2+(u+2v+1)^2-(2u+2v+1)^2 = 4\left(v^2-\tfrac{1}{2}u(u+1)\right)$$

we obtain a solution of the equation $x^2+(x+1)^2 = z^2$ and $u = z-x-1$, $v = \frac{1}{2}(2x+1-z)$. As we have seen, these formulae transform all solutions of the equation $x^2+(x+1)^2 = z^2$ in natural numbers x, z into all the solutions of equation (18) in natural numbers u and v, or, equivalently, into all the triangular numbers which are squares of natural numbers. It follows that there are infinitely many triangular numbers of this kind. We present here the first six triangular numbers which are the squares of natural numbers obtained from the first six solutions in natural numbers of the equation $x^2+(x+1)^2 = z^2$:

$$t_1 = 1^2, \quad t_8 = 6^2, \quad t_{49} = 35^2, \quad t_{288} = 204^2, \quad t_{1681} = 1189^2,$$
$$t_{9800} = 6930^2.$$

It follows from the identity

$$(19) \qquad (2z-2x-1)^2-2(2x-z+1)^2-1 = 2\left(z^2-x^2-(x+1)^2\right)$$

that if natural numbers x, z satisfy equation (12), then, setting

$$(20) \qquad a = 2z-2x-1, \qquad b = 2x-z+1,$$

we obtain

$$(21) \qquad a^2-2b^2 = 1,$$

where a, b are natural numbers; in fact, since, in virtue of (12), we have $z < 2x+1$, also $4z^2 > (2x+1)^2$, whence $2z > 2x+1$.

Formulae (20) are, obviously, equivalent to the following ones:

$$(22) \qquad x = b+\tfrac{1}{2}(a-1), \qquad z = a+b.$$

If numbers a and b are natural and satisfy equation (21), then a is plainly an odd number greater than 1, and the numbers given by (22) are natural. Moreover, since (20) implies (22), then, in virtue of (21), (20) and (19), we see that the numbers x and z satisfy equation (12).

From this we conclude that from the set of all the solutions in natural numbers x, z of equation (12) we obtain, using formulae (20), all the solutions of equation (21) in natural numbers a and b.

For example, the first four solutions just presented of equation (12) give the following solutions (a,b) of equation (21):(3,2), (17, 12), (99, 70) (577, 408).

Conversely, from all the solutions of equation (21) in natural numbers we obtain, using formulae (22), all the solutions in natural numbers of equation (12).

5. Pythagorean triangles of the same area

From the list of Pythagorean triangles presented in § 1 we infer that the triangles (21, 20, 29) and (35, 12, 37) have the same area (= 210) and that these are the two least primitive Pythagorean triangles with different hypotenuses and the same area. Taking into account non-primitive triangles with hypotenuses $\leqslant 37$ we obtain other 8 triangles (6, 8, 10), (9, 12, 15), (12, 16, 20), (15, 20, 25), (10, 24, 26), (18, 24, 30), (30, 16, 34), (21, 28, 35) of area 24, 54, 96, 150, 120, 216, 240, 294, respectively. Thus we see that there is no pair of triangles among the Pythagorean triangles with hypotenuses $\leqslant 37$ such that both triangles of the pair have the same area, except the pair (21, 20, 29), (35, 12, 37).

We note that two Pythagorean triangles of the same area and the equal hypotenuses are congruent. In fact, if (a_1, b_1, c_1) and (a_2, b_2, c_2) are such triangles and $a_1 \geqslant b_1$, $a_2 \geqslant b_2$, then, by hypothesis, $a_1 b_1 = a_2 b_2$ and $c_1 = c_2$, whence $a_1^2+b_1^2 = a_2^2+b_2^2$ consequently, $(a_1-b_1)^2 = (a_2-b_2)^2$ and $(a_1+b_1)^2 = (a_2+b_2)^2$, whence $a_1-b_1 = a_2-b_2$ and $a_1+b_1 = a_2+b_2$, which implies $a_1 = a_2$ and $b_1 = b_2$, as asserted. From the list in § 3 we select the Pythagorean triangle (15, 112, 113), whose area is $840 = 4 \cdot 210$. This area is 4 times greater than the area of the triangles (21, 20, 29) and (35, 12, 37). Thus multiplying each side of each of these triangles by 2 we obtain the triangles (42, 40, 58) and (70, 24, 74) respectively with the area equal to 840. So we have obtained three Pythagorean triangles

$$(15,\ 112,\ 113), \quad (42,\ 40,\ 58), \quad (70,\ 24,\ 74)$$

all having the same area.

Not all of these triangles are of course primitive. It is known that the least number being the common value of the area of three primitive Pythagorean triangles is 13123110 and the triangles are

$$(4485,\ 5852,\ 7373), \quad (19019,\ 1390,\ 19069),$$
$$(3059,\ 8580,\ 9089).$$

The generators of the corresponding solutions of the Pytaghorean equation are (39, 38), (138, 5), (78, 55), respectively.

It is of some interest to know whether there exist arbitrarily large systems of Pythagorean triangles with different hypotenuses and the same area.

The answer to this question is given by the following theorem of Fermat.

THEOREM 2. *For every natural number n there exist n Pythagorean triangles with different hypotenuses and the same area.*

This theorem follows by induction from the following

LEMMA. *If we are given n Pythagorean triangles with different hypotenuses and the same area and if for at least one of the triangles the hypotenuse is odd, then we can construct $n+1$ Pythagorean triangles with different hypotenuses and the same area such that for at least one of the triangles the hypotenuse is odd.*

PROOF. Let n be a given natural number. Suppose (a_k, b_k, c_k) with $a_k < b_k < c_k$, $k = 1, 2, \ldots, n$, are n given Pythagorean triangles, all having the same area, and such that c_k's, $k = 1, 2, \ldots, n$, are all different and c_1 is odd. Set

$$a'_k = 2c_1(b_1^2 - a_1^2)a_k, \quad b'_k = 2c_1(b_1^2 - a_1^2)b_k, \tag{23}$$
$$c'_k = 2c_1(b_1^2 - a_1^2)c_k, \quad \text{for } k = 1, 2, \ldots, n$$

and

$$(24)\quad a'_{n+1} = (b_1^2 - a_1^2)^2, \quad b'_{n+1} = 4a_1 b_1 c_1^2, \quad c'_{n+1} = 4a_1^2 b_1^2 + c_1^4.$$

For $k = 1, 2, \ldots, n$ the triangles (a'_k, b'_k, c'_k) are plainly Pythagorean triangles, since they are similar to the triangles (a_k, b_k, c_k), $k = 1, 2, \ldots, n$, respectively. But also $(a'_{n+1}, b'_{n+1}, c'_{n+1})$ is a Pythagorean triangle. This follows immediately from (24), the equation $a_1^2 + b_1^2 = c_1^2$ and from the easily verifiable identity

$$(b^2 - a^2)^4 + 16a^2b^2(a^2 + b^2)^2 = \left(4a^2b^2 + (a^2 + b^2)^2\right)^2.$$

We now prove that the triangles (a'_k, b'_k, c'_k), where $k = 1, 2, \ldots, n+1$, satisfy the remaining conditions.

Let Δ be the area of each of the triangles (a_k, b_k, c_k), $k = 1, 2, \ldots, n$. We then have $a_k b_k = 2\Delta$ for $k = 1, 2, \ldots, n$. The area of the triangle (a'_k, b'_k, c'_k) with $k = 1, 2, \ldots, n$ is, by (23), equal to $\frac{1}{2}a'_k b'_k = 2c_1^2(b_1^2 - a_1^2)^2 a_k b_k = 4c_1^2(b_1^2 - a_1^2)^2\Delta$. The area of the triangle $(a'_{n+1}, b'_{n+1}, c'_{n+1})$ is, by (24), equal to $\frac{1}{2}a'_{n+1} b'_{n+1} = 2(b_1^2 - a_1^2)^2 c_1^2 a_1 b_1 = 4c_1^2(b_1^2 - a_1^2)^2\Delta$. Thus the triangles (a'_k, b'_k, c'_k), where $k = 1, 2, \ldots, n+1$, have the same area.

To see that the hypotenuses of the triangles (a'_k, b'_k, c'_k), where $k = 1, 2, \ldots, n$, are all different, we note that numbers c_k, $k = 1, 2, \ldots, n$, as the hypotenuses of the triangles (a_k, b_k, c_k) are all different. Besides, by (23), c'_k $(k \leqslant n)$ are all even numbers. On the other hand, in virtue of (24), the number c'_{n+1} is odd, since c_1 is odd. Thus we have proved that the numbers c'_k, where $k = 1, 2, \ldots, n+1$, are all different. This completes the proof of the lemma. □

The simplest special case of the lemma is obtained for $n = 1$. The least Pythagorean triangle to which the lemma can be applied is, of course, the triangle (3, 4, 5). Using the lemma we obtain the following two triangles of the same area: (a'_1, b'_1, c'_1) and (a'_2, b'_2, c'_2), where, according to formulae (23), by the equality $2(b_1^2-a_1^2)c_1 = 2\cdot 7\cdot 5 = 70$, we have $a'_1 = 3\cdot 70 = 210$, $b'_1 = 4\cdot 70 = 280$, $c'_1 = 5\cdot 70 = 350$ and, in virtue of formulae (24), $a'_2 = (4^2-3^2)^2 = 49$, $b'_2 = 4\cdot 3\cdot 4\cdot 5^2 = 1200$, $c'_2 = 4\cdot 3^2\cdot 4^2+5^4 = 1201$. This gives us two Pythagorean triangles, (210, 280, 350) and (49, 1200, 1201), with different hypotenuses (and one of them odd) and the same area equal to 29400. Applying the lemma again to the triangles just obtained we obtain three Pythagorean triangles with different hypotenuses and the same area, the sides of which, however, are all greater than 10^{10}. On the other hand, by the use of different methods we have already found three relevant Pythagorean triangles whose sides are less than 10^4. There exist also four Pythagorean triangles with different hypotenuses and the same area whose sides are less than 10^5. These are (518, 1320, 1418), (280, 2442, 2458), (231, 2960, 2969), (111, 6160, 6161) and the area of each of them is 314880. And here are five Pythagorean triangles of this kind with side less than 10^6: (2805, 52416, 52491), (3168, 46410, 46518), (5236, 14040, 28564), (6006, 24480, 25206), (8580, 17136, 19164); the area of each of them is 73513440.

Of course there exist only finitely many Pythagorean triangles with a given area Δ; for the catheti of such a triangle must be divisors of the number 2Δ. On the other hand, it follows easily from the lemma proved above that *there exist infinitely many non-congruent rectangular triangles whose sides are rational and areas equal to* 6.

In fact, it follows from the proof of the lemma that if we are given n Pythagorean triangles with different hypotenuses, one of them odd, and such that the area of each of the triangles is Δ, then there exist $n+1$ Pythagorean triangles with different hypotenuses, one of them odd, and such that the area of each of the triangles is Δd^2, where d is a natural number. Starting with the triangle (3, 4, 5) and applying the lemma $n-1$ times we obtain n Pythagorean triangles with different hypotenuses, the area of each being equal to $6m^2$, where m is a natural number (depending on n). Dividing the sides of these triangles by m we obtain n non-congruent rectangular triangles whose sides are rational and areas equal to 6. Since n was an arbitrary natural number, we see that the number of non-congruent rectangular triangles whose sides are rational and areas equal to 6 cannot be finite, so there are infinitely many such triangles, as asserted.

We note that it is easy to prove that for each natural number n there exist $\geqslant n$ mutually non-congruent Pythagorean triangles having perimeters of the same length.

In fact, no two non-congruent primitive Pythagorean triangles are similar. but the number of them is, as we know, infinite. Let us take n such non-congruent triangles (a_k, b_k, c_k) $(k = 1, 2, \dots, n)$ and set $a_k + b_k + c_k = s_k$ for $k = 1, 2, \dots, n$. Let

$$s = s_1 s_2 \dots s_n, \quad a'_k = \frac{a_k s}{s_k}, \quad b'_k = \frac{b_k s}{s_k}, \quad c'_k = \frac{c_k s}{s_k} \quad \text{for } k = 1, 2, \dots, n.$$

We then have $a'_k + b'_k + c'_k = s$ for $k = 1, 2, \dots, n$ and, moreover, no two of the Pythagorean triangles (a'_k, b'_k, c'_k) $(k = 1, 2, \dots, n)$ are similar; consequently, they are not congruent.

The list of all the primitive Pythagorean triangles with perimeters less than 10000 in length has been given by A. A. Krishnawami [1]. Two triangles missing in this list have been found by D. H. Lehmer [5]. In particular, the number of triangles with perimeters not greater than 1000 in length is 70, and there are 703 triangles with perimeters not greater than 10000 in length.

It is easy to prove that for each natural number s there exist a primitive Pythagorean triangle whose perimeter length is the sth power of a natural number. In fact, let t be a natural number $\geqslant s > 1$ and let $m = 2^{s-1}t^s$, $n = (2t-1)^s - m$. Since, in view of $t \geqslant s$, we have

$$\left(1 - \frac{1}{2t}\right)^s \geqslant \left(1 - \frac{1}{2s}\right)^s \geqslant 1 - \frac{s}{2s} = \frac{1}{2},$$

then, using $s > 1$, we observe that $(2t-1)^s > 2^{s-1}t^s$. Consequently n is a natural number and it is less than m (since $(2t-1)^s < 2^s t^s = 2m$).

It is obvious that $(m, n) = 1$. Now finding the numbers x, y, z from formulae (9) we obtain a Pythagorean triangle whose perimeter length is the number $x+y+z = 2m(m+n) = [2t(2t-1)]^s$. For $s = 2$ we obtain the triangle (63, 16, 65), whose perimeter length is 12^2.

It is easy to find all the Pythagorean triangles whose areas are equal to their perimeter lengths (see de Comberousse [1], pp. 190-191). The sides x, y, z of such a triangle must satisfy the equations

$$x^2+y^2 = z^2 \quad \text{and} \quad x+y+z = \tfrac{1}{2}xy.$$

Eliminating z we obtain the equation

$$(x-4)(y-4) = 8. \tag{25}$$

This implies that $x-4\mid 8$. We cannot have $x-4 < 0$, because in the case $x-4 = -1$ or $x-4 = -2$ we would have $y-4 = -8$ or $y-4 = -2$, respectively; this, in turn, would give $y = -4$ or $y = 0$, which is obviously impossible. But if $x-4 = -4$ or $x-4 = -8$, then $x \leqslant 0$, which is also impossible. Thus we conclude that $x-4 > 0$ and therefore, by $x-4\mid 8$, we see that $x-4 = 1, 2, 4$ or 8, whence $x = 5, 6, 8$ or 12. Consequently, using (25), we obtain $y = 12, 8, 6$ or 5. This leads us to the conclusion that there are precisely two non-congruent relevant triangles, namely (5, 12, 13) and (6, 8, 10). The area and the length of the perimeter of the first is 30, of the other 24.

It is easy to prove that there exist infinitely many Pythagorean triangles whose sides are rational and areas equal to the lengths of their perimeters. It can be proved that all such triangles (u, v, w) are given by the formulae

$$u = \frac{2(m+n)}{n}, \qquad v = \frac{4m}{m-n}, \qquad w = \frac{2(m^2+n^2)}{(m-n)n},$$

where m and $n < m$ are natural numbers.

6. On squares whose sum and difference are squares

Now we consider the problem of existence of natural numbers x, y, z, t satisfying the following system of equations

$$x^2+y^2 = z^2, \qquad x^2-y^2 = t^2. \tag{26}$$

In other words, we are going to answer the question whether there exist two natural numbers x and y such that the sum and the difference of their squares are squares. The answer is given by the following theorem of Fermat.

THEOREM 3. *There are no two natural numbers such that the sum and the difference of their squares are squares.*

PROOF. Suppose that there exist natural numbers x and y such that $x^2+y^2 = z^2$ and $x^2-y^2 = t^2$, where z and t are natural numbers and, of course, $z > t$. Among all the pairs x, y there exists a pair for which the number x^2+y^2 is the least. Let x, y denote such a pair. We must have $(x, y) = 1$. For if $d \mid x$ and $d > y$ with $d \mid 1$, then, in virtue of $x^2+y^2 = z^2$, $x^2-y^2 = t^2$, we would have $d^2 \mid z^2$, $d^2 \mid t^2$, whence $d \mid z$ and $d \mid t$, but this would imply that the equation can be divided throughout by d^2, contrary to the assumption that x, y denote the solution for which the sum x^2+y^2 is the least. It follows from (26) that $2x^2 = z^2+t^2$. Therefore the numbers z and t are both odd or both even. Hence the numbers $z+t$ and $z-t$ are both even and therefore $\frac{1}{2}(z+t)$ and $\frac{1}{2}(z-t)$ are natural numbers. If $d \mid \frac{1}{2}(z+t)$ and $d \mid \frac{1}{2}(z-t)$ and d is greater than 1, then $d \mid z$, which in virtue of

$$x^2 = \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2, \tag{27}$$

implies $d^2 \mid x^2$ and so $d \mid x$. Consequently, since $x^2+y^2 = z^2$, we also have $d \mid y$, which is clearly impossible since $(x, y) = 1$.

Thus

$$\left(\frac{z+t}{2}, \frac{z-t}{2}\right) = 1. \tag{28}$$

From (28) and (27) we infer that the numbers $\frac{1}{2}(z+t)$, $\frac{1}{2}(z-t)$, x form a primitive solution of the Pythagorean equation, which by Theorem 1, implies that there exist relatively prime natural numbers m, n with $m > n$, one of them even and the other odd, for which either

$$\tfrac{1}{2}(z-t) = m^2-n^2, \quad \tfrac{1}{2}(z+t) = 2mn$$

or

$$\tfrac{1}{2}(z+t) = m^2-n^2, \quad \tfrac{1}{2}(z-t) = 2mn$$

hold. Since $2y^2 = z^2-t^2$, in either case we have

$$2y^2 = 2(m^2-n^2)4mn, \quad \text{whence} \quad y^2 = (m^2-n^2)4mn.$$

As the number y is even, $y = 2k$, where k is a natural number. Using the formulae for y^2 we obtain

$$(m^2-n^2)mn = k^2. \tag{29}$$

Since $(m, n) = 1$, we have $(m \pm n, m) = 1$, whence $(m^2 - n^2, m) = 1$ and $(m^2 - n^2, n) = 1$. From (29) we infer that, according to the corollary of Theorem 8 of Chapter I, each of the numbers $m^2 - n^2$, m, n is the square of a natural number, thus $m = a^2$, $n = b^2$, $m^2 - n^2 = c^2$, where a, b, c are natural numbers. From $(m, n) = 1$ and from the fact that one of the numbers m, n is even and the other is odd we infer that $(m+n, m-n) = 1$. In fact, every common divisor of the odd numbers $m+n$ and $m-n$ is odd, but it is also a divisor of the numbers $2m$ and $2n$, thus, since $(m, n) = 1$, it equals to 1. From the equalities $(m+n, m-n) = 1$ and $(m+n)(m-n) = m^2 - n^2 = c^2$ (by the already mentioned corollary) it follows that the numbers $m+n$ and $m-n$ are squares. Thus, since $m = a^2$, $n = b^2$, the numbers a^2+b^2 and a^2-b^2 are squares. But $a^2+b^2 = m+n < 2m \leqslant 2mn \leqslant \frac{1}{2}(z+t) < z \leqslant z^2 = x^2+y^2$, whence $a^2+b^2 < x^2+y^2$, contrary to the assumption concerning the pair x, y.

Thus the assumption that there exist natural numbers for which the sum and the difference of their squares are squares leads to a contradiction. This completes the proof of Theorem 3. □

On the other hand, there exist infinitely many pairs of natural numbers x, y for which there exist natural numbers z and t such that $x^2+y^2 = z^2+1$ and $x^2-y^2 = t^2+1$. For instance, if q is even then for $x = \frac{q^4}{2}+1$, $y = q^3$ we have

$$x^2+y^2 = (q^2+q^4/2)^2+1, \qquad x^2-y^2 = (q^4/2-q^2)^2+1.$$

We also have $(2n^2)^2 \pm (2n)^2 = (2n^2 \pm 1)^2 - 1$ for $n = 1, 2, \ldots$ There exist other pairs of natural numbers x, y such that for some natural numbers z, t we have $x^2+y^2 = z^2-1$, $x^2-y^2 = t^2-1$, e.g. $21^2+12^2 = 14^2-1$, $21^2-12^2 = 10^2-1$. It is not difficult to see that there exist pairs of natural numbers x, y for which we can find natural numbers z, t such that $x^2+y^2 = z^2+1$ and $x^2-y^2 = t^2-1$, e.g. $13^2+11^2 = 17^2+1$, $13^2-11^2 = 7^2-1$ or $89^2+79^2 = 119^2+1$, $89^2-79^2 = 41^2-1$.

It follows from Theorem 3 that *the system of equations*

$$(*) \qquad x^2+y^2 = u^2, \qquad x^2+2y^2 = v^2$$

has no solutions in natural numbers x, y, u, v.

In fact, if for some natural numbers x, y, u, v formulae $(*)$ hold, then $u^2+y^2 = v^2$, $u^2-y^2 = x^2$, contrary to Theorem 3.

COROLLARY 1. *There are no natural numbers a, b, c such that $a^4 - b^4 = c^2$.*

PROOF. If the numbers a, b, c could be found, then we might assume that $(a, b) = 1$; for, if $(a, b) = d > 1$, then putting $a = da_1$, $b = db_1$ we would have $d^4(a_1^4 - b_1^4) = c^2$, whence $d^2 \mid c$, so $c = d^2 c_1$ and therefore $a_1^4 - b_1^4 = c_1^2$, where $(a_1, b_1) = 1$. Thus assuming $(a, b) = 1$, we have $(a^2, b^2) = 1$, whence in virtue of the equality $b^4 + c^2 = a^4$, the numbers b^2, c, a^2 form a primitive solution of the Pythagorean equation. Then from Theorem 1 we infer that there exist natural numbers m, n, $m > n$, such that $a^2 = m^2 + n^2$ and either $b^2 = m^2 - n^2$ or $b^2 = 2mn$. The first case is impossible, since it contradicts Theorem 3. In the second case we have $a^2 + b^2 = (m+n)^2$ and $a^2 - b^2 = (m-n)^2$, which also contradicts Theorem 3. This completes the proof of Corollary 1. ☐

It follows that *there are no natural numbers for which the sum and the difference of their squares are both the k-th multiples of squares of natural numbers*, for otherwise we would have $a^4 - b^4 = (kuv)^2$, contrary to Corollary 1.

By Corollary 1 the difference of the fourth powers of natural numbers is not the square of a natural number; the product, however, of two different differences of this kind can be the square of a natural number; for instance

$$(3^4 - 2^4)(11^4 - 2^4) = 975^2, \qquad (2^4 - 1^4)(23^4 - 7^4) = 2040^2,$$
$$(5^4 - 4^4)(21^4 - 20^4) = 3567^2, \qquad (9^4 - 7^4)(11^4 - 2^4) = 7800^2.$$

COROLLARY 2. *There are no natural numbers x, y, z satisfying the equation $x^4 + y^4 = z^4$* (this is the *Fermat Last Theorem* for the exponent 4, cf. § 18).

PROOF. If the numbers x, y, z existed, then we would have $z^4 - y^4 = (x^2)^2$, contrary to Corollary 1. ☐

Corollary 2 can also be expressed by saying that there is no Pythagorean triangle whose sides are squares.

K. Zarankiewicz has asked whether there exists a Pythagorean triangle whose sides are triangular numbers (i.e. numbers $t_n = n(n+1)/2$).

The answer to this question is obtained simply by checking that the numbers $t_{132} = 8778$, $t_{143} = 10296$, $t_{164} = 13530$ form a Pythagorean triangle. We do not know whether there exist any other Pythagorean triangle with this property. However, there exist infinitely many Pythagorean triangles whose catheti are consecutive triangular numbers. As a matter of fact, in § 4 we have proved that the equation $x^2 + (x$

$+1)^2 = z^2$ has infinitely many solutions in natural numbers x, z. For each such solution x, z, we easily check that $t_{2x}^2 + t_{2x+1}^2 = [(2x+1)z]^2$. For example we have $t_6^2 + t_7^2 = 35^2$, $t_{40}^2 + t_{41}^2 = (41 \cdot 29)^2$. It is known that there exist infinitely many primitive Pythagorean triangles whose catheti are triangular numbers. To this class belongs the triangle $(t_7, t_9, 53)$.

If for some natural numbers a, b, c we have $t_a^2 + t_b^2 = t_c^2$, then, as can easily be verified, we also have $((2a+1)^2-1)^2 + ((2b+1)^2-1)^2 = ((2c+1)^2-1)^2$. Thus the equation $(x^2-1)^2+(y^2-1)^2 = (z^2-1)^2$ has a solution in odd natural numbers x, y, z, namely $x = 263$, $y = 287$, $z = 329$. The equation has also another solution in which not all numbers x, y, z are odd, e.g. $x = 10$, $y = 13$, $z = 14$. We do not know whether this equation has infinitely many solutions in natural numbers > 1.

It is easy to prove that there is no primitive Pythagorean triangle such that adding 1 to its hypotenuse we obtain the square of a natural number. In fact, the hypotenuse of a primitive Pythagorean triangle is, by theorem 1, of the form $m^2 + n^2$, where one of the numbers m, n is even and the other is odd; consequently, dividing the number $m^2 + n^2 + 1$ by 4, we obtain the remainder 2, whence we infer that $m^2 + n^2 + 1$ cannot be the square of a natural number.

It is easy to prove that the equation

$$(x^2-1)^2+(y^2-1)^2 = (z^2+1)^2$$

has infinitely many solutions in natural numbers x, y, z. This follows immediately from the identity

$$((2n^2+2n)^2-1))^2+((2n+1)^2-1)^2 = ((2n^2+2n)^2+1)^2$$

for $n = 1, 2, \ldots$, which, in particular, gives $(4^2-1)^2+(3^2-1)^2 = (4^2+1)^2$, $(12^2-1)^2+(5^2-1)^2 = (12^2+1)^2$, $(24^2-1)^2+(7^2-1)^2 = (24^2+1)^2$. We note that the numbers $2n^2+2n$ and $2n+1$ can always be regarded as the catheti of a Pythagorean triangle, for

$$(2n^2+2n)^2+(2n+1)^2 = (2n^2+2n+1)^2 \qquad \text{for } n = 1, 2, \ldots$$

Also the equation

$$(x^2-1)^2+(y^2)^2 = (z^2-1)^2$$

has infinitely many solutions in natural numbers. This follows from the identity

$$((8n^4-1)^2-1)^2+((2n)^6)^2 = ((8n^4+1)^2-1)^2 \qquad \text{for} \qquad n = 1, 2, \ldots$$

Thus, in particular, $(7^2-1)^2+(8^2)^2 = (9^2-1)^2$.

However, there is no Pythagorean triangle for which by subtracting 1 from each of its catheti we would obtain the squares of natural numbers. The reason is that, as we know, in each Pythagorean triangle at least one of the catheti is divisible by 4.

It can be proved that for each Pythagorean triangle (a, b, c) and for each natural number n there exists a triangle similar to the triangle (a, b, c) and such that each of its sides is the mth power of a natural number with $m \geqslant n$. To construct this triangle it is sufficient to multiply each of the sides of the triangle (a, b, c) by $a^{2(4n^2-1)}b^{4n(n-1)(2n+1)}c^{4n^2(2n-1)}$. Using the fact that $a^2+b^2 = c^2$, one easily sees that

$$\left(\left(a^{2n}b^{(n-1)(2n+1)}c^{n(2n-1)}\right)^{2n}\right)^2+\left(\left(a^{2n+1}b^{2n^2-1}c^{2n^2}\right)^{2n-1}\right)^2$$
$$= \left(\left(a^{2n-1}b^{2(n-1)n}c^{2n^2-2n+1}\right)^{2n+1}\right)^2.$$

Thus in particular for $n = 2$, if $a^2+b^2 = c^2$, then

$$((a^4b^5c^6)^4)^2+((a^5b^7c^8)^3)^2 = ((a^3b^4c^5)^5)^2.$$

It is not known whether there exist natural numbers x, y, z, t such that $x^4+y^4+z^4 = t^4$. It is known that the equation has no solutions in natural numbers x, y, z, t with t less than 220000 (Lander, Parkin and Selfridge [1]). It is interesting to know that $30^4+120^4+274^4+315^4 = 353^4$ (Norrie, 1911) and $133^4+134^4 = 59^4+158^4$ (Euler, 1778). We do not know whether the equation $x^4+y^4+z^4+t^4 = u^4$ has infinitely many solutions in natural numbers x, y, z, t, u such that $(x, y, z, t) = 1$. Apart from the solution mentioned above there are precisely 81 other solutions of this equation with $u \leqslant 20469$ and $(x, y, z, t) = 1$ (Rose and Brudno [1]), e.g. $240^4+340^4+430^4+599^4 = 651^4$ (J. O. Patterson 1942).

On the other hand, there exist infinitely many quadruples x, y, z, t such that $(x, y, z, t) = 1$ and $x^4+y^4 = z^4+t^4$ (cf. Lander and Parkin [1], Lander, Parkin and Selfridge [1], Zajta [1]).

We also have

$$2^4+2^4+3^4+4^4+4^4 = 5^4,$$
$$4^4+6^4+8^4+9^4+14^4 = 15^4,$$
$$1^4+8^4+12^4+32^4+64^4 = 65^4.$$

Turning back to Corollary 1 we note that the equation $x^4-y^4 = z^3$ has solutions in natural numbers. In fact, for a natural number k we have

$$(k(k^4-1)^2)^4-((k^4-1)^2)^4 = ((k^4-1)^3)^3.$$

Thus, in particular, for $k = 2$, $450^4-225^4 = (15^3)^3$. E. Swift [1] has proved that the equation $x^4-y^4 = z^3$ has no solutions in natural numbers x, y, z such that $(x, y) = 1$.

COROLLARY 3. *There are no three squares forming an arithmetical progression whose difference is a square.*

PROOF. If for natural numbers x, y, z, t the equalities $y^2-x^2 = t^2$ and $z^2-y^2 = t^2$ were valid, then $y^2-t^2 = x^2$, $y^2+t^2 = z^2$, contrary to Theorem 3. ☐

COROLLARY 4 (Theorem of Fermat). *There is no Pythagorean triangle whose area is the square of a natural number* (¹).

PROOF. Suppose, to the contrary, that such a triangle (a, b, c) exists. Then $a^2+b^2 = c^2$ and $ab = 2d^2$, where d and c are natural numbers. Without loss of generality we may assume that $a > b$, since the case $a = b$ could not possibly occur because $2a^2 = c^2$ is impossible. Hence $c^2+(2d)^2 = (a+b)^2$, $c^2-(2d)^2 = (a-b)^2$, contrary to Theorem 3. ☐

We leave to the reader an easy proof of the fact that there are no two rationals, each different from zero, such that the sum and the difference of their squares are the squares of rational numbers.

Similarly, it is not difficult to prove that there are no rational numbers a, b, c, all different from zero, such that $a^4-b^4 = c^2$.

To see this we suppose, on the contrary, that such numbers a, b, c exist. We may of course assume that they are all positive. So $a = l/m$, $b = r/s$, $c = u/v$, where l, m, r, s, u, v are natural numbers. Since $a^4-b^4 = c^2$, we see that $(lvs)^4-(rvm)^4 = (uvm^2s^2)^2$, contrary to Corollary 1.

It can easily be proved that there are no squares of rational numbers, all different from zero, which form an arithmetical progression in which the difference is the square of a rational number. It follows that there is no rational number x for which each of the numbers $x, x+1, x+2$ is the square of a rational number.

(¹) C. M. Walsh devoted a long paper to this theorem [1]. The paper contains detailed historical references as well as many remarks by the author himself.

7. The equation $x^4+y^4 = z^2$

It seems to be a natural question to ask whether there exist Pythagorean triangles in which both catheti are squares. The answer to this question is given by the following theorem of Fermat and is negative.

THEOREM 4. *The equation*

$$x^4+y^4 = z^2 \tag{30}$$

has no solutions in natural numbers x, y, z.

PROOF. Suppose, on the contrary, that equation (30) has a solution in natural number and let z denote the least natural number which square is the sum of the fourth powers of two natural numbers x, y. We have $(x, y) = 1$; for, otherwise, i.e. when $(x, y) = d > 1$, we would have $x = dx_1$, $y = dy_1$, x_1, y_1 being natural numbers, whence $z^2 = d^4(x_1^4+y_1^4)$, and consequently $d^4 \mid z^2$, which, as we know, would imply $d^2 \mid z$, so $z = d^2z_1$, z_1 being a natural number. Therefore, by (30) $x_1^2+y_1^2 = z_1^2 < z^2$, contrary to the assumption regarding z. Thus, since $(x, y) = 1$ implies $(x^2, y^2) = 1$, the numbers x^2, y^2, z form a primitive solution of the Pythagorean equation

$$(x^2)^2+(y^2)^2 = z^2. \tag{31}$$

In view of Theorem 1 one of the numbers x^2 and y^2, say y^2, is even and

$$x^2 = m^2-n^2, \qquad y^2 = 2mn, \qquad z = m^2+n^2, \tag{32}$$

where $(m, n) = 1$, $m > n$, one of the numbers m, n being even and the other odd. If m is even and n is odd then in the Pythagorean equation $x^2+n^2 = m^2$, as a consequence of (32), both x and n are odd. But the last statement leads to a contradiction. In fact, in virtue of what we proved in § 3, the square of an odd number divided by 8 leaves the remainder 1, consequently, the left-hand side of the equation $x^2+n^2 = m^2$ divided by 8 would give the remainder 2 and hence it could not be a square. Thus m is odd and $n = 2k$, where k is a natural number. Since $(m, n) = 1$, we have $(m, k) = 1$. Then, from the second equality of (32), we conclude that $y^2 = 2^2mk$, consequently y is even so $y = 2l$, whence $l^2 = mk$. Since $(m, k) = 1$, by Theorem 8 of Chapter I, the numbers m and k are the squares of natural numbers, i.e. $m = a^2$, $k = b^2$, where a, b are natural numbers. We have $n = 2k = 2b^2$. Hence, by (32), $x^2+n^2 = m^2$, which in virtue of $(m, n) = 1$ implies $(x, n) = 1$. Therefore the numbers x, n, m form a primitive solution of the Pythagorean equation, which, in view of Theorem 1 and the fact that n is even, implies that

$$(33)\qquad n = 2m_1 n_1, \qquad m = m_1^2+n_1^2,$$

where m_1, n_1 are relatively prime natural numbers.

Since $n = 2b^2$, we have $b^2 = m_1 n_1$, whence, from $(m_1, n_1) = 1$, we infer that the numbers m_1, n_1 are squares, so $m_1 = a_1^2$, $n_1 = b_1^2$ and since $m = a^2$, using (33) we conclude that $a^2 = m_1^2+n_1^2 = a_1^4+b_1^4$. But $a \leqslant a^2 = m < m^2+n^2 = z$, whence $a < z$, contrary to the assumption regarding z. Thus the assumption that equation (30) has solutions in natural numbers leads to a contradiction. This completes the proof of Theorem 4. □

It follows from Theorem 4 that there are no Pythagorean triangles in which both catheti are squares. It could also be proved that there is no Pythagorean triangle in which both catheti are cubes, but the proof is much more difficult.

With reference to Theorem 4 we notice that

$$12^4+15^4+20^4 = 481^2.$$

More generally, it can be proved that if $x^2+y^2 = z^2$, then

$$(34)\qquad (xy)^4+(xz)^4+(yz)^4 = (z^4-x^2y^2)^2.$$

If $(x, y) = (x, z) = (y, z) = 1$, then, as one easily can prove, $(xy, xz, yz) = 1$. Therefore from (34), in view of the fact that there exist infinitely many primitive solutions of the Pythagorean equation, we infer that the equation

$$t^4+u^4+v^4 = w^2$$

has infinitely many solutions in natural numbers t, u, v, w, with $(t, u, v) = 1$.

We note that $2^4+4^4+6^4+7^4 = 63^2$. Moreover, as we have shown in § 5, the sum of four biquadrates can be the fourth power of a natural number. On the other hand, we are unable to prove or disprove Euler's conjecture that the sum of three biquadrates cannot be the fourth power of a natural number.

In connection with the above we note that the system of equations

$$x^4+y^4+z^4 = 2t^4, \qquad x^2+y^2+z^2 = 2t^2$$

has infinitely many solutions in natural numbers x, y, z, t.

We deduce this from the identities

$$(n^2-1)^4+(2n\pm 1)^4+(n^2\pm 2n)^4 = 2(n^2\pm n+1)^4,$$

$$(n^2-1)^2+(2n\pm 1)^2+(n^2\pm 2n)^2 = 2(n^2\pm n+1)^2,$$

and the identities

$$(4n)^4+(3n^2-1)^4+(3n^2-2n-1)^4 = 2(3n^2+1)^4,$$

$$(4n)^2+(3n^2+2n-1)^2+(3n^2-2n-1)^2 = 2(3n^2+1)^2.$$

In particular,

$$3^4+5^4+8^4 = 2\cdot 7^4, \qquad 3^2+5^2+8^2 = 2\cdot 7^2,$$

$$7^4+8^4+15^4 = 2\cdot 13^4, \qquad 7^2+8^2+15^2 = 2\cdot 13^2.$$

With reference to Theorem 4 we note that the equation $x^4+y^4 = 2z^2$ has trivial solutions in natural numbers, namely $x = y, z = x^2$, x being an arbitrary natural number. As was shown by Legendre, these are the only solutions of this equation in natural numbers. In fact, if we could have $x^4+y^4 = 2z^2$ for some natural numbers x, y, z with $x \neq y$, say $x > y$, then the numbers x, y would both be even or both odd. Consequently, $a = \frac{1}{2}(x^2+y^2)$ and $b = \frac{1}{2}(x^2-y^2)$ would be natural numbers. Hence $x^2 = a+b$, $y^2 = a-b$, $2z^2 = x^4+y^4 = 2(a^2+b^2)$ and, consequently, $a^2+b^2 = z^2$, $a^2-b^2 = (xy)^2$, contrary to Theorem 3.

It follows that *there are no three different natural numbers whose fourth powers form an arithmetical progression.*

(The proof that there are no three cubes forming an arithmetical progression is more difficult, cf. § 14.)

It is easy to see that the equation $x^4+y^4 = 3z^2$ has no solutions in natural numbers. This is because the equation $x^2+y^2 = 3z^2$ is not soluble in natural numbers.

Also the equation $x^4+y^4 = 4z^2$ is insoluble in natural numbers. To see this we write it in the form $x^4+y^4 = (2z)^2$ and use Theorem 4. Similarly $x^4+y^4 = 9z^2$ is insolvable in natural numbers.

We now prove that the equation $x^4+y^4 = 5z^2$ has no solutions in natural numbers. We may, clearly, suppose that neither of the numbers x, y is divisible by 5, consequently each of them is either of the form $5k\pm 1$ or $5k\pm 2$. Since $(5k\pm 1)^2 = 5(5k^2\pm 2k)+1$, $(5k\pm 2)^2 = 5(5k^2\pm 4k+1)-1$, we conclude that the square of each of the numbers x, y is of the form $5k\pm 1$. Therefore, dividing the fourth power of each of the numbers x, y by 5, we obtain the remainder 1. Consequently, dividing x^4+y^4 by 5, we obtain the remainder 2, thus $x^4+y^4 = 5z^2$ does not hold.

It can also be proved that if k is a natural number $\neq 8$ such that $3 \leqslant k \leqslant 16$, then the equation $x^4+y^4 = kz^2$ is insolvable in natural numbers. On the other hand, the equation $x^4+y^4 = 17z^4$ has a solution in natural numbers namely $x = 2$, $y = z = 1$. The equation $x^4+y^4 = 8z^2$ has only a trivial solution in natural numbers, namely $x = y = 2k$, where k is a natural number, $z = x^2/2$.

It follows from the identity

$$(a^3-3ab^2)^2+(3a^2b-b^3)^2 = (a^2+b^2)^3$$

that the equation $x^2+y^2 = z^3$ has infinitely many solutions in natural numbers x, y, z. It is easy to prove that the numbers

$$x = 8n(n^2-4), \qquad y = n^4-24n^2+16, \qquad z = n^2+4,$$

where n is an odd natural number > 1, are relatively prime and satisfy the equation $x^2+y^2 = z^4$.

8. On three squares for which the sum of any two is a square

Given a solution x, y, z in natural numbers of the Pythagorean equation. We put

$$(35) \qquad a = x(4y^2-z^2), \qquad b = y(4x^2-z^2), \qquad c = 4xyz.$$

Since $x^2+y^2 = z^2$, we have

$$a^2+b^2 = z^6, \qquad a^2+c^2 = x^2(4y^2+z^2)^2, \qquad b^2+c^2 = y^2(4x^2+z^2)^2.$$

Thus from a given solution of the Pythagorean equation in natural numbers we obtain natural numbers a, b, c such that the sum of the squares of any two of them is the square of a natural number. The numbers a, b, c are then the sides of a rectangular parallelepiped such that the diagonals of its faces are natural numbers.

In particular, putting $x = 3$, $y = 4$, $z = 5$ we find

$$a = 117, \qquad b = 44, \qquad c = 240, \qquad a^2+b^2 = 125^2, \qquad a^2+c^2 = 267^2,$$
$$b^2+c^2 = 244^2.$$

These numbers were found by P. Halcke in 1719.

It can be proved that there exist natural numbers a, b, c for which the sums of the squares of any two of them are squares and which cannot be obtained from any solution of the Pythagorean equation by the use of formulae (35). In particular, this is the case with $a = 252$, $b = 240$, $c = 275$, $a^2+b^2 = 348^2$, $a^2+c^2 = 373^2$, $b^2+c^2 = 365^2$; for, c cannot be equal to $4xyz$, and, on the other hand, since $x < z$, $y < z$, the value for c must be the greatest of the values for a, b, c obtained from (35).

As we know, in a solution u, v, w of the equation $u^2+v^2 = w^2$ at least one of the numbers u, v is divisible by 3 and at least one is divisible by 4. Therefore, if the sum of the squares of any two of the numbers a, b, c is a square, then at least two of the numbers a, b, c must be divisible by 3 and at least two of them must be divisible by 4. (Otherwise, if, for instance, the numbers a and b were not divisible by 3, then the sum of the squares of them would not be a square.) Consequently not all pairs formed from the numbers a, b, c obtained from (35) are relatively prime. It can be proved, however, that if x, y, z is a primitive solution of the Pythagorean equation, then for the numbers a, b, c obtained from (35) we have $(a, b) = 1$. This proves that there exist infinitely many systems of the numbers a, b, c such that $(a, b, c) = 1$ and that the sum of the squares of any two of them is a square.

It is easy to prove that if a, b, c are natural numbers such that the sum of the squares of any two of them is a square, then the numbers ab, ac, bc have the same property.

M. Kraïtchik devoted to the search of such triples a, b, c Chapters IV–VI of his book [3], see also Leech [2], Korec [1].

We do not know whether there exist three natural numbers a, b, c such that each of the numbers

$$a^2+b^2,\quad a^2+c^2,\quad b^2+c^2\quad\text{and}\quad a^2+b^2+c^2$$

is the square of a natural number. In other words, we do not know whether there exist a rectangular parallelepiped whose sides, face diagonals and inner diagonal are all natural numbers.

On the other hand, there exist three natural numbers a, b, c, e.g. $a = 124$, $b = 957$, $c = 13852800$, such that each of the numbers a^2+b^2, a^2+c, b^2+c and a^2+b^2+c is a perfect square (Bromhead [1]).

There exist four natural numbers x, y, z, t such that the sum of the squares of any three of them is a square. S. Tebay (cf. Dickson [7], vol. II, p. 505) has found the following formulae for the numbers of this kind:

$$x = (s^2-1)(s^2-9)(s^2+3),\qquad y = 4s(s-1)(s+3)(s^2+3),$$
$$z = 4s(s+1)(s-3)(s^2+3),\qquad t = 2s(s^2-1)(s^2-9),$$

where s is a natural number greater than 3. It can be calculated that

$$x^2+y^2+z^2 = ((s^2+3)(s^4+6s^2+9))^2,$$
$$x^2+y^2+t^2 = ((s-1)(s+3)(s^4-2s^3+10s^2+6s+9))^2,$$

$$x^2+z^2+t^2 = ((s-1)(s-3)(s^4+2s^3+10s^2-6s+9))^2,$$
$$y^2+z^2+t^2 = (2s(3s^4+2s^3+27))^2.$$

In particular, for $s = 4$ we obtain $x = 1995$, $y = 6384$, $z = 1520$, $t = 840$. Euler found a solution $x = 168$, $y = 280$, $z = 105$, $t = 60$, which cannot be obtained from the above mentioned formulae (see also Jean Lagrange [1]). Euler was interested in finding three natural numbers x, y, z for which each of the numbers $x \pm y$, $x \pm z$, $y \pm z$ is the square of a natural number. He gave the following example of such numbers:

$$x = 434657, \qquad y = 420968, \qquad z = 150568.$$

Infinitely many such triples of coprime integers x, y, z are known (cf. Dickson [7], vol. II, p. 449).

To conclude this section we prove that *there exists an infinite sequence of natural numbers* $a_1, a_2, \ldots$ *such that each of the numbers* $a_1^2+a_2^2+\ldots+a_n^2$, *where* $n = 1, 2, \ldots$, *is the square of a natural number.*

We proceed by induction. Suppose that for a natural number n the numbers $a_1, a_2, \ldots, a_n$ have already been defined in such a manner that $a_1^2+a_2^2+\ldots+a_n^2$ is the square of an odd natural number > 1. So

$$a_1^2+a_2^2+\ldots+a_n^2 = (2k+1)^2,$$

where k is a natural number. Of course for $n = 1$ we can take $a_1 = 3$. Then, using the identity

$$(2k+1)^2+(2k^2+2k)^2 = (2k^2+2k+1)^2,$$

and putting $a_{n+1} = 2k^2+2k$, we obtain

$$a_1^2+a_2^2+\ldots+a_{n+1}^2 = (2k^2+2k+1)^2,$$

which again is the square of an odd natural number. Thus the assertion follows.

Putting $a_1 = 3$ we have $a_2 = 4$, $a_3 = 12$, $a_4 = 84$, $a_5 = 3612$ and so on. Thus

$$3^2+4^2 = 5^2, \qquad 3^2+4^2+12^2 = 13^2, \qquad 3^2+4^2+12^2+84^2 = 85^2,$$
$$3^2+4^2+12^2+84^2+3612^2 = 3613^2.$$

9. Congruent numbers

A natural number h is called *congruent* if there exists (at least one) rational number v such that each of the numbers v^2+h, v^2-h is the square of a rational number.

Suppose that h is a congruent number. Then there exist natural numbers a, b, c such that $z^2+hc^2 = a^2$, $z^2-hc^2 = b^2$. We have, of course, $a > b$ and $2z^2 = a^2+b^2$. It follows that both a and b are either even or odd. Hence both $a+b$ and $a-b$ are even, and thus $a+b = 2x$, $a-b = 2y$, where x, y are natural numbers. We have $a = x+y$, $b = x-y$ and, consequently, $2z^2 = a^2+b^2 = (x+y)^2+(x-y)^2 = 2x^2+2y^2$, whence $z^2 = x^2+y^2$. Moreover, in virtue of the equalities $z^2+hc^2 = a^2$, $z^2-hc^2 = b^2$, we have $2hc^2 = a^2-b^2 = (x+y)^2-(x-y)^2 = 4xy$, whence $hc^2 = 2xy$. Thus, if h is a congruent number, then there exists a solution of the equation $x^2+y^2 = z^2$ in natural numbers x, y, z such that $hc^2 = 2xy$. Conversely, if natural numbers x, y, z satisfy the equation $x^2+y^2 = z^2$, then, as it can be easily checked, $z^2 \pm 2xy = (x \pm y)^2$. We sum up the above-mentioned results in the following statement:

Every solution of the equation $x^2+y^2 = z^2$ *in natural numbers* x, y, z *defines a congruent number* $h = 2xy$. *Conversely, every congruent number can be obtained in this way, by taking out a square factor.*

The least solution of the Pythagorean equation in natural numbers, 3, 4, 5, gives the congruent number which is $2\cdot 3\cdot 4 = 24 = 2^2\cdot 6$ (we have here $5^2+24 = 7^2$, $5^2-24 = 1^2$). The solution (5, 12, 13) gives the congruent number $2\cdot 5\cdot 12 = 120 = 2^2\cdot 30$ (here $13^2+120 = 17^2$, $13^2-120 = 7^2$). The non-primitive solution (6, 8, 10) gives the congruent number $96 = 4^2\cdot 6$ (here $10^2+96 = 14^2$, $10^2-96 = 2^2$). The solution (8, 15, 17) gives the congruent number $240 = 4^2\cdot 15$ (here $17^2+240 = 23^2$, $17^2-240 = 7^2$). The solution (9, 40, 41) gives the congruent number $720 = 12^2\cdot 5$, here $41^2+720 = 49^2$, $41^2-720 = 31^2$. Dividing both sides of these equalities by 12^2 we obtain

$$\left(\frac{41}{12}\right)^2+5 = \left(\frac{49}{12}\right)^2, \quad \left(\frac{41}{12}\right)^2-5 = \left(\frac{31}{12}\right)^2.$$

The following problem dates from about 1220: find a rational number r such that both r^2+5 and r^2-5 are the squares of rational numbers. The answer, found approximately about the same date was $r = \frac{41}{12}$. There exists also another solution, which was found in 1931 by J.D. Hill [1]. This is $r = \frac{3344161}{1494696}$. Here

$$r^2+5 = \left(\frac{4728001}{1494696}\right)^2, \quad r^2-5 = \left(\frac{113279}{1494696}\right)^2.$$

J. V. Uspensky and M.A. Heaslet [1] (pp. 419-427) have proved that the above two solutions are the solutions with the least denominators.

They have found another solution, in which the denominator and the numerator have 15 digits each, and have also presented a method for finding all the solutions which are infinite in number.

We present here the proof that there exist infinitely many rational numbers r for which each of the numbers r^2+5, r^2-5 is the square of a rational number.

Suppose that $r = x/y$, where x, y are natural numbers such that y is even, $(x, y) = 1$ and each of the numbers r^2+5 and r^2-5 is the square of a rational number. Each of the numbers $(x^2+5y^2)/y^2$ and $(x^2-5y^2)/y^2$ is the square of a rational number; consequently, the same is true for the numbers x^2+5y^2 and x^2-5y^2. But, since these are natural numbers, they are squares of natural numbers, so $x^2+5y^2 = z^2$, $x^2-5y^2 = t^2$.

Put

$$r_1 = \frac{x^4+25y^4}{2xyzt}. \tag{36}$$

An obvious computation shows that

$$r_1^2 \pm 5 = \left(\frac{x^4 \pm 10x^2y^2 - 25y^4}{2xyzt}\right)^2.$$

$x_1 = x^4+25y^4$ and $y_1 = xyzt$ are natural numbers and y_1 is even and greater than y. It can be proved that $(x_1, y_1) = 1$.

Thus for each rational number r which is an irreducible fraction x/y, where x is a natural number, y is an even integer, and is such that both r^2+5 and r^2-5 are squares of rational numbers, by (36) we obtain another rational number r_1, having the above-mentioned properties and such that its denominator is greater than y. It follows that there exist infinitely many rational numbers r for which both r^2+5 and r^2-5 are squares of rational numbers. Starting with the number $r = \frac{41}{12}$, found by Leonardo Pisano (Fibonacci), by (36) we obtain the number $r_1 = \frac{3344161}{1494696}$, found by Hill. Then, applying (36) to the number r_1, we obtain the number r_2, whose numerator has 27 digits. As we have already mentioned, Uspensky and Heaslet have found a rational number r such that both r^2+5 and r^2-5 are squares of rational numbers and such that its numerator has 15 digits. From this we see that by the successive use of formula (36) we do not obtain all the rational numbers r for which r^2+5 and r^2-5 are squares of rational numbers, though we get infinitely many of them.

The reason why people have been interested in finding rational numbers r for which $r^2 \pm 5$ are the squares of rational numbers seems to lie in the fact that for natural numbers $h < 5$ there are no rational numbers r for which $r^2 \pm h$ are squares of rational numbers. The proof of this for $h = 1$ and $h = 4$ follows immediately from Theorem 3.

The proof for $h = 2$ is somewhat more difficult. Suppose that for a rational number r the numbers r^2+2 and r^2-2 are the squares of rational numbers. If $r = x/y$, where x, y are natural numbers, then the numbers x^2+2y^2 and x^2-2y^2 are squares of rational numbers. Hence, since they are natural numbers, they are squares of integers, and thus there exist integers z and t such that $x^2+2y^2 = z^2$, $x^2-2y^2 = t^2$. Hence $2x^2 = z^2+t^2$, $4y^2 = z^2-t^2$, whence $4x^2 = (z+t)^2+(z-t)^2$. Consequently, $[2x(z-t)]^2 = (z^2-t^2)^2+(z-t)^4 = (2y)^4+(z-t)^4$. But, since $z \neq t$, this contradicts Theorem 4.

The proof for $h = 3$ is more difficult.

On the other hand, we have

$$\left(\frac{5}{2}\right)^2+6 = \left(\frac{7}{2}\right)^2, \quad \left(\frac{5}{2}\right)^2-6 = \left(\frac{1}{2}\right)^2, \quad \left(\frac{337}{120}\right)^2+7 = \left(\frac{463}{10}\right)^2,$$
$$\left(\frac{337}{120}\right)^2-7 = \left(\frac{113}{120}\right)^2.$$

A table of congruent numbers less than 1000 is given in Tunnel [1].

It is easy to prove that there are no natural numbers x, y, such that x^2+y and $x+y^2$ are squares of natural numbers. In fact, if $x^2+y = t^2$, where x, y, t are natural numbers, then $t > x$ and consequently $t \geqslant x+1$, whence $t^2 \geqslant x^2+2x+1$. Therefore $y = t^2-x^2 \geqslant 2x+1 > x$ and also $x > y$, which is impossible.

On the other hand, there exist infinitely many positive rational numbers x, y, for which the numbers x^2+y and $x+y^2$ are squares of rational numbers. In fact, for $x = (n^2-8n)/16(n+1)$, $y = 2x+1$, where n is a natural number > 8, x, y are positive rational numbers and we have

$$x^2+y = \left(\frac{n^2+8n+16}{16(n+1)}\right)^2, \quad x+y^2 = \left(\frac{n^2+2n-8}{8(n+1)}\right)^2.$$

Turning back to congruent numbers we note that, in view of their above-mentioned connection with the solutions of the Pythagorean equation and by the formulae for the solutions of the Pythagorean equation in natural numbers presented in § 3, *in order that a number h be a congruent number it is necessary and sufficient that*

$$hc^2 = 4mn(m^2-n^2)l^2,$$

where c, m, n, l are natural numbers, $(m, n) = 1$, $m > n$, *and* $2 | mn$.

We then have

$$((m^2+n^2)l)^2 \pm hc^2 = ((m^2-n^2 \pm 2mn)l)^2.$$

If h is a congruent number, $z^2+hc^2 = a^2$, $z^2-hc^2 = b^2$, then the numbers b^2, z^2, a^2 form an arithmetical progression with the difference hc^2. Conversely, if numbers b^2, z^2, a^2 form an arithmetical progression with the difference hc^2, then h is a congruent number. Thus *a congruent number can be defined up to a square factor as the difference of an arithmetical progression consisting of three terms, all being squares of natural numbers.*

It follows that every arithmetical progression of this kind is of the form

$$l^2(m^2-n^2-2mn)^2, \quad l^2(m^2+n^2)^2, \quad l^2(m^2-n^2+2mn)^2,$$

where m, n are natural numbers and $m > n$.

It can be proved that *in order for a natural number k there exist a natural number x such that* $k+x^2$ *and* $k-x^2$ *are squares of natural numbers it is necessary and sufficient that* $k = (4m^4+n^4)l^2$, *where m, n, l are natural numbers.* (Without loss of generality we may suppose that the numbers m, n are relatively prime.)

For $m = n = 1$ we have $5+2^2 = 3^2$, $5-2^2 = 1^2$,

for $m = 1, n = 2$ we have $20+4^2 = 6^2$, $20-4^2 = 2^2$,

for $m = 2, n = 1$ we have $65+4^2 = 9^2$, $65-4^2 = 7^2$,

for $m = 1, n = 3$ we have $85+6^2 = 11^2$, $85-6^2 = 7^2$.

10. The equation $x^2+y^2+z^2 = t^2$

We are going to find all the solutions in natural numbers of the equation

$$(37) \qquad x^2+y^2+z^2 = t^2.$$

First of all we note that at least two of the numbers x, y, z must be even. Suppose to the contrary that all three numbers x, y, z are odd. Then t^2, being the sum of the squares of x, y, z, is a number of the form $8k+3$, since, as we know, dividing the square of each of the odd numbers x, y, z by 8, we obtain the remainder 1. But this very fact applied to t^2, which is again the square of an odd number, leads to a contradiction. If only one of the numbers x, y, z were even, the sum $x^2+y^2+z^2 = t^2$ would be of the form $4k+2$, which is impossible, since the square of an even number is of the form $4k$.

Suppose that the numbers y and z are even. So

$$y = 2l, \qquad z = 2m, \tag{38}$$

where l and m are natural numbers. From (37) we see that $t > x$. Setting

$$t-x = u \tag{39}$$

we obtain a natural number u for which, by (37), (38), (39), we have

$$(x+u)^2 = x^2+4l^2+4m^2,$$

whence, after a trivial reduction, we obtain $2xu+u^2 = 4l^2+4m^2$, and further

$$u^2 = 4l^2+4m^2-2xu. \tag{40}$$

The right-hand side of equality (40), as the algebraic sum of even numbers, is even. Therefore u^2 and, consequently, u are even. So

$$u = 2n, \tag{41}$$

where n is a natural number. Substituting (41) in (40) and dividing the equation thus obtained throughout by 4 we see that

$$n^2 = l^2+m^2-nx.$$

The last equation can be rewritten in the form

$$x = \frac{l^2+m^2-n^2}{n}, \tag{42}$$

which, in view of (39), implies

$$t = x+u = x+2n = \frac{l^2+m^2+n^2}{n}.$$

Moreover, since x is a natural number, from (42) we conclude that $n^2 < l^2+m^2$. Thus we have proved that all the solutions of equation (37) in natural numbers x, y, z, t, with even y, z, can be obtained from the formulae

$$(43)\quad x = \frac{l^2+m^2-n^2}{n}, \qquad y = 2l, \qquad z = 2m, \qquad t = \frac{l^2+m^2+n^2}{n},$$

where m, n, l are natural numbers and n is a divisor of the sum l^2+m^2 less than $\sqrt{l^2+m^2}$.

We now prove that, conversely, if l, m, n satisfy the above conditions, then the numbers x, y, z, t obtained from (43) form a solution of equation (37) in natural numbers. The fact that x, y, z, t are natural numbers is an immediate consequence of the conditions. To see that they satisfy equation (37) we use the identity

$$\left(\frac{l^2+m^2-n^2}{n}\right)^2 + (2l)^2 + (2m)^2 = \left(\frac{l^2+m^2+n^2}{n}\right)^2.$$

It is easy to prove hat every solution of equation (37) in natural numbers x, y, z, t with even y, z is obtained exactly once by the use of formulae (43). For, by (43) we have

$$l = \frac{y}{2}, \qquad m = \frac{z}{2}, \qquad n = \frac{t-x}{2},$$

and thus the numbers l, m, n are defined uniquely by x, y, z, t. The above argument proves the following

THEOREM 5. *All the solutions of the equation*

$$x^2+y^2+z^2 = t^2$$

in natural numbers x, y, z, t, with even y, z, are obtained from the formulae

$$x = \frac{l^2+m^2-n^2}{n}, \qquad y = 2l, \qquad z = 2m, \qquad t = \frac{l^2+m^2+n^2}{n},$$

l, m being arbitrary natural numbers, and n being the divisors of l^2+m^2 less than $\sqrt{l^2+m^2}$. Every solution is obtained exactly once in this way.

Theorem 5 not only states the existence of the solutions of equation (37) but also gives a method for finding them. It is easy to see that in order to eliminate the solutions with interchanged unknowns we may reject the pairs l, m for which $m > l$ and take only those n for which the numbers x are odd. But thus we eliminate also all the solutions for which x, y, z, t are even. To include them again it is sufficient to multiply each of the solutions with odd x by the powers of 2, successively.

Here are the first ten solutions of equation (37) obtained in this way:

l	m	l^2+m^2	n	x	y	z	t
1	1	2	1	1	2	2	3
2	2	8	1	7	4	4	9
3	1	10	1	9	6	2	11
3	1	10	2	3	6	2	7
3	3	18	1	17	6	6	19
3	3	18	2	7	6	6	11
3	3	18	3	3	6	6	9
4	2	20	1	19	8	4	21
4	2	20	4	1	8	4	9
4	4	32	1	31	8	8	33

It is worth-while to notice that, as has been proved by R. D. Carmichael [4], pp. 39–43, all the solutions of equation (37) in natural numbers can be obtained from the identity

$$d^2(m^2-n^2-p^2+q^2)^2+d^2(2mn-2pq)^2+d^2(2mp+2nq)^2$$
$$= d^2(m^2+n^2+p^2+q^2)^2.$$

11. The equation $xy = zt$

Suppose that natural numbers x, y, z, t, satisfy the equation $xy = zt$ and let $(x, z) = a$. Then $x = ac$, $z = ad$, where c and d are natural numbers and $(c, d) = 1$. Hence $acy = adt$, i.e. $cy = dt$ and, since $(c, d) = 1$, we observe that $d \mid y$; consequently $y = bd$, where b is a natural number, whence $t = bc$. This proves that if natural numbers x, y, z, t satisfy the equation $xy = zt$, then there exist natural numbers a, b, c, d such that $(c, d) = 1$ and $x = ac$, $y = bd$, $z = ad$, $t = bc$. It is evident that if, conversely, for given natural numbers a, b, c, d we define x, y, z, t by the above formulae, then $xy = zt$. Thus we have proved the following

THEOREM 6. *All the solutions of the equation $xy = zt$ in natural numbers x, y, z, t are given by the formulae*

$$x = ac, \qquad y = bd, \qquad z = ad, \qquad t = bc,$$

where a, b, c, d are arbitrary natural numbers. Moreover, this remains true when an additional condition $(c, d) = 1$ is postulated.

It is easy to prove that if the additional condition $(c, d) = 1$ is satisfied, then the above formulae for x, y, z, t give each of the solutions exactly once.

In order to obtain the solutions of the equation $xy = zt$, we could also proceed as follows: we start with arbitrary natural numbers x, z. Then, since the numbers $\frac{x}{(x,z)}$, $\frac{z}{(x,z)}$ are relatively prime, in virtue of the equality $\frac{x}{(x,z)}y = \frac{z}{(x,z)}t$ we have $\frac{z}{(x,z)} \mid y$; consequently $y = \frac{uz}{(x,z)}$, whence $t = \frac{ux}{(x,z)}$. On the other hand, taking arbitrary natural numbers for x, z, u and putting $y = \frac{uz}{(x,z)}$, $t = \frac{ux}{(x,z)}$, we obtain a solution of the equation $xy = zt$ in natural numbers. Thus, all the solutions of the equation $xy = tz$ in natural numbers are given by the formulae $y = \frac{uz}{(x,z)}$, $t = \frac{ux}{(x,z)}$, where x, z, u are arbitrary natural numbers.

It is worth-while to note that if natural numbers x, y, z, t satisfy the equation $xy = zt$, then $x = (x,z)(x,t):(x,y,z,t)$.

It can easily be proved that *all the solutions of the equation* $xy = z^2$ *in natural numbers* x, y, z *are given by the formulae* $x = u^2t$, $y = v^2t$, $z = uvt$, *where* u, v, t *are arbitrary natural numbers. We may assume additionally that* $(u,v) = 1$; *then each solution is obtained exactly once from the above-mentioned formulae.*

It can be proved that *all the solutions of the equation* $xy = z^3$ *in natural numbers* x, y, z *are given by the formulae* $x = uv^2t^3$, $y = u^2vw^3$, $z = uvtw$, *where* u, v, t, w *are arbitrary natural numbers.*

More generally, there are corresponding formulae for the solutions in natural numbers $x_1, x_2, \ldots, x_n$, z of the equation $x_1 x_2 \ldots x_n = z^k$ in which $n \geqslant 2$ and k is a natural number (Ward [1], cf. Schinzel [4]).

It is easy to prove that *for given natural numbers* n *and* m *all the solutions of the equation* $x_1 x_2 \ldots x_n = y_1 y_2 \ldots y_m$ *in natural numbers* $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots y_m$ *are given by the formulae*

$$x_n = \frac{y_1 y_2 \ldots y_{m-1} t}{(x_1 x_2 \ldots x_{n-1}, y_1 y_2 \ldots y_{m-1})}, \quad y_m = \frac{x_1 x_2 \ldots x_{n-1} t}{(x_1 x_2 \ldots x_{n-1}, y_1 y_2 \ldots y_{m-1})},$$

where $x_1, x_2, \ldots, x_{n-1}$, $y_1, y_2, \ldots, y_{m-1}$, t *are arbitrary natural numbers.*

Here are some other formulae for the solutions of the last equation in which mn arbitrary natural parameters t_{ij} $(i = 1, 2, \ldots, m, j = 1, 2, \ldots, n)$ are involved. These are

$$y_i = t_{i,1} t_{i,2} \ldots t_{i,n} \quad (i = 1, 2, \ldots, m),$$

$$x_j = t_{1,j} t_{2,j} \ldots t_{m,j} \quad (j = 1, 2, \ldots, n).$$

The proof of the fact that for arbitrary natural values of the parameters $t_{i,j}$, $i = 1, 2, ..., m$, $j = 1, 2, ..., n$, the formulae give a solution of equation $x_1 x_2 ... x_n = y_1 y_2 ... y_m$ is straightforward. However, the proof that all the solutions are obtained in this way is complicated (Bell [1]).

EXERCISES. 1. Find all the solutions of the equation $(x+y+z)^3 = x^3+y^3+z^3$ in integers x, y, z.

SOLUTION. In view of the identity

$$(x+y+z)^3-(x^3+y^3+z^3) = 3(x+y)(y+z)(z+x)$$

it suffices to solve in integers the equation

$$(x+y)(y+z)(z+x) = 0$$

But this we do simply by taking arbitrary integers for any two of the unknowns x, y z and one of the already chosen integers with the opposite sign for the remaining unknown.

2. Find all the solutions of the system of equation

$$x+y+z = t, \quad x^2+y^2+z^2 = t^2, \quad x^3+y^3+z^3 = t^3 \tag{44}$$

in integers x, y, t, z.

SOLUTION. It follows from equations (44) that $xy+yz+zx = 0$ and $(x+y)(y+z)(x+z) = 0$ (compare exercise 1). If for instance $x+y = 0$, then, in virtue of $xy+yz+zx = xy+(x+y)z = 0$, we infer that $xy = 0$, whence $x = y = 0$. Hence, if the integers x, y, z, t satisfy the system of equations (44), then two of the numbers x, y, z must be equal to zero; the third is equal to t, where t is an arbitrary integer. Thus system (44) has no solutions apart from the trivial ones.

3. Find all the pairs of natural numbers x, y for which the number xy is divisible by $x+y$.

SOLUTION. All such pairs are given by the formulae

$$x = k(m+n)m, \quad y = k(m+n)n, \tag{45}$$

where k is an arbitrary natural number and m, n are relatively prime. It follows from (45) that $xy/(x+y) = kmn$; consequently $x+y \mid xy$. On the other hand, if for natural numbers x, y, $x+y \mid xy$ holds, then, putting $d = (x,y)$, $x = dm$, $y = dn$, we obtain $(m, n) = 1$ and $d(m+n) \mid d^2mn$, whence $m+n \mid dmn$. Further, since $(m, n) = 1$, we have $(m+n, mn) = 1$. Consequently $m+n \mid d$, and so $d = k(m+n)$ where k is a natural number. Hence, in virtue of $x = dm$ and $y = dn$, we obtain formulae (45).

It is also easy to prove that for natural numbers k, m, n with $(m, n) = 1$ every pair x, y of natural numbers satisfying the condition $x+y \mid xy$ is obtained precisely once from formulae (45).

In fact, in view of formulae (45), we observe that, since $(m, n) = 1$, $\frac{m}{n}$ is an irreducible fraction equal to $\frac{x}{y}$. Consequently, the numbers x, y define the numbers m, n uniquely. So, in virtue of (45), the number k is also defined uniquely by the numbers x, y.

4. Find all the solutions of the equation

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{z} \tag{46}$$

in natural numbers x, y, z.

SOLUTION. All the solutions of equation (46) in natural numbers x, y, z are given by the formulae

$$x = k(m+n)m, \quad y = k(m+n)n, \quad z = kmn, \tag{47}$$

where k is a natural number and $(m, n) = 1$. In fact, if natural numbers x, y, z satisfy equation (46), then $(x+y)z = xy$, whence $x+y \mid xy$ and in virtue of exercise 3 we see that formulae (45) are valid for x, y. Therefore $z = xy/(x+y) = kmn$, which gives formulae (47). On the other hand, it is easy to check that the numbers x, y, z obtained from formulae (47) satisfy equation (46).

5. Find all the solutions of the equation

$$(x+y+z)^2 = x^2+y^2+z^2 \tag{48}$$

in integers x, y, z.

SOLUTION. Equation (48) is clearly equivalent to the equation

$$xy+yz+zx = 0. \tag{49}$$

If integers x, y, z satisfy equation (49) and at least one of them, say x, is equal to zero, then by (49) $yz = 0$, which proves that also one of the numbers z, y is then equal to zero. Thus, if one of the numbers x, y, z satisfying equation (48) is equal to zero, then at least two of those numbers are equal to zero. On the other hand, if two of the numbers x, y, z equal zero and the third is an arbitrary integer, then, clearly, equation (48) is satisfied.

Therefore, in what follows we assume that none of the numbers x, y, z is equal to zero. Then, by (49), two of those numbers must be either both positive or both negative and the remaining one must have the opposite sign. Thus, changing if necessary the signs of the numbers x, y, z (which do not affect the equation), we may assume that $x > 0, y > 0, z < 0$. From equation (49) we infer that $xy = -(x+y)z$. This proves that $x+y \mid xy$. But then we can apply formulae (45) of exercise 3, which give $z = -\frac{xy}{x+y} = -kmn$. Thus, if integers x, y, z satisfy equation (48), $x > 0, y > 0$, then, for some natural numbers k, m, n with $(m, n) = 1$, we obtain

$$x = k(m+n)m, \quad y = k(m+n)n, \quad z = -kmn. \tag{50}$$

On the other hand, a straightforward computation shows that for all natural numbers k, m, n formulae (50) give a solution of equation (48). Therefore, all the solutions of equation (45) in integers x, y, z with $x > 0, y > 0$ are given by formulae (50), where k, m, n are natural numbers. Moreover, we may confine our attention only to the case where $(m, n) = 1$.

From this all the solutions of equation (48) in integers x, y, z can easily be found.

6. Prove the equivalence of the following two statements:

(i) there exist positive integers a, b, c, d, e, f, g such that

$$a^2+b^2 = e^2, \quad b^2+c^2 = f^2, \quad a^2+c^2 = g^2, \quad a^2+b^2+c^2 = d^2 \tag{51}$$

(ii) there exist rational numbers x, y, z greater than 1 such that

$$\left(\frac{x}{1+x^2}\right)^2+\left(\frac{v}{1+y^2}\right)^2=\left(\frac{z}{1+z^2}\right)^2. \tag{52}$$

PROOF (found by M. Skałba). (i) → (ii). Assume without loss of generality that $(a,b,c,d)=1$. It follows that d is odd and exactly one of the numbers a, b, c is odd, let it be a. From Theorem 1 and (51) it follows that there exist positive integers d_i, m_i, n_i $(i=1,2,3)$ such that

$$a=d_1(m_1^2-n_1^2);\quad b=d_2\,2m_2n_2,\quad c=d_3\,2m_3n_3,$$

$$d=d_i(m_i^2+n_i^2)\quad\text{for}\quad i=1,2,3. \tag{53}$$

The equality $a^2+b^2+c^2=d^2$ takes the form

$$(d_2m_2n_2)^2+(d_3m_3n_3)^2=(d_1m_1n_1)^2.$$

If we divide both sides by $d^2=d_i^2(m_i^2+n_i^2)^2$ we get (52) with

$$x=\frac{m_2}{n_2}>1,\quad y=\frac{m_3}{n_3}>1,\quad z=\frac{m_1}{n_1}>1$$

(ii) → (i). Let rational numbers x, y, z greater than 1 satisfy (52). Writing

$$x=\frac{m_2}{n_2},\quad y=\frac{m_3}{n_3},\quad z=\frac{m_1}{n_1},$$

where m_i, n_i are positive integers, let us put

$$d=\prod_{i=1}^{3}(m_i^2+n_i^2).$$

If we define d_i $(i=1,2,3)$ and then a, b, c by the formulae (53) and if we take

$$e=d_3(m_3^2-n_3^2),\quad f=d_1 2m_1n_1,\quad g=d_2(m_2^2-n_2^2),$$

we get positive integers a, b, c, d, e, f, g satisfying (51).

12. The equation $x^4-x^2y^2+y^4=z^2$

The equation

$$x^4-x^2y^2+y^4=z^2 \tag{54}$$

has an obvious solution in natural numbers $x=y$, $z=y^2$, where y is an arbitrary natural number. Suppose that x, y, z is a solution of equation (54) in natural numbers with $x\neq y$. Clearly, we may suppose that $(x,y)=1$, since otherwise, i.e. when $(x,y)=d>1$, we have $x=dx_1$, $y=dy_1$, whence, in virtue of (54), $d^4\mid z^2$, and so $z=dz_1^2$. Dividing (54) throughout by d^4, we obtain $(x_1,y_1)=1$ and $x_1^4-x_1^2y_1^2+y_1^4=z_1^2$. Let x, y, z be a solution of equation (54) in natural numbers such that $(x,y)=1$ and $x\neq y$. Moreover, suppose that for the solution x, y, z the product xy takes the least possible value.

We now suppose that one of the numbers x, y, say y, is even. Since $(x, y) = 1$, x must be odd. Equation (54) can be rewritten in the form $(x^2-y^2)^2+(xy)^2 = z^2$ with $x^2-y^2 \neq 0$ (since $x \neq y$). It follows from the relation $(x, y) = 1$ that $(x^2-y^2, xy) = 1$. Moreover, since the number xy is even, by the formulae for primitive solutions of the Pythagorean equation we see that there exist natural numbers m, n, such that $(m, n) = 1, 2 \mid mn, x^2-y^2 = m^2-n^2, xy = 2mn$. Since x is odd and y is even, the number x^2-y^2 and hence the number m^2-n^2 is of the form $4k+1$, which shows that m cannot be even and n odd. Therefore n must be even and m odd. Let $y = 2y_0$, where y_0 is a natural number. By $xy = 2nm$ we find $xy_0 = mn$, where $(x, y_0) = (m, n) = 1$. In virtue of Theorem 6 there exist natural numbers a, b, c such that $x = ac$, $y_0 = bd$, $m = ad$, $n = bc$ with $(c, d) = 1$. Since $(x, y_0) = (m, n) = 1$, then, clearly, any two of the numbers a, b, c, d are relatively prime. Since the numbers x, m are odd, the numbers a, c, d are odd, whence, since n is even, b must be even. Substituting $x = ac$, $y = 2y_0 = 2bd$, $m = ad$, $n = bc$ in the equation $x^2-y^2 = m^2-n^2$, we obtain $(a^2+b^2)c^2 = (a^2+4b^2)d^2$. Let $\delta = (a^2+b^2, a^2+4b^2)$. We have $\delta \mid a^2+4b^2-(a^2+b^2) = 3b^2$ and $\delta \mid 4(a^2+b^2)-(a^2+4b^2) = 3a^2$, whence, in view of $(a, b) = 1$, $\delta \mid 3$. But number 3 is not a divisor of the number a^2+b^2; for, the relation $3 \mid a^2+b^2$ together with the relation $(a, b) = 1$ would imply that neither of the numbers a, b is divisible by 3, which in turn would imply that by dividing the sum of the squares of the numbers a, b by 3 we would obtain the remainder 2, which contradicts the fact that $3 \mid a^2+b^2$. Thus $\delta = 1$, i.e. $(a^2+b^2, a^2+4b^2) = 1$, whence the equality $(a^2+b^2)c^2 = (a^2+4b^2)d^2$ implies the relations $a^2+b^2 \mid d^2$ and $c^2 \mid a^2+4b^2$. On the other hand, $(c, d) = 1$ implies that $d^2 \mid a^2+b^2$ and $c^2 \mid a^2+4b^2$. Hence $a^2+b^2 = d^2$ and $a^2+4b^2 = c^2$. But $(a, b) = 1$ and equivalently, since a is odd, $(a, 2b) = 1$. Therefore, in virtue of the formulae for primitive solutions of the Pythagorean equation, the equality $a^2+(2b)^2 = c^2$ implies the existence of natural numbers x_1, y_1 such that $(x_1\, y_1) = 1, 2 \mid x_1\, y_1, a = x_1^2-y_1^2, b = x_1\, y_1$. We have $a^2+b^2 = d^2$. Hence $x_1^4-x_1^2\, y_1^2+y_1^4 = d^2$, and one of the numbers x_1, y_1 is even. But $x_1\, y_1 = b < 2bd = y \leqslant xy$, whence $x_1\, y_1 < xy$, contrary to the assumption regarding the solution x, y, z.

This proves that both the numbers x, y must be odd. Since $x \neq y$, we may suppose that $x > y$. Since $(x^2-y^2)^2+(xy)^2 = z^2$ and the number $x^2-y^2 > 0$ is even, there exist natural numbers m, n such that $(m, n) = 1$, $2 \mid mn$, $x^2-y^2 = 2mn$, and $xy = m^2-n^2$. Consequently,

$$m^4-m^2n^2+n^4 = (m^2-n^2)^2+m^2n^2$$

$$= (xy)^2+\left(\frac{x^2-y^2}{2}\right)^2 = \left(\frac{x^2+y^2}{2}\right)^2$$

and $(m, n) = 1$, one of the numbers m, n being even. But this, as was proved before, is impossible.

Thus we have proved the following

THEOREM 7. *The equation* $x^4-x^2y^2+y^4 = z^2$ *has no solutions in natural numbers* x, y, z *apart from the trivial one* $x = y$, $z = x^2$.

The proof of the theorem presented above is due to H. C. Pocklington [1]. From the theorem just proved Pocklington derives the following theorem of Fermat.

THEOREM 8. *There are no four different squares which form an arithmetical progression.*

PROOF. Suppose to the contrary that x^2, y^2, z^2, w^2 are natural numbers and that $y^2-x^2 = z^2-y^2 = w^2-z^2$. Hence $2y^2 = x^2+z^2$, $2z^2 = y^2+w^2$ and, consequently, $2y^2w^2 = x^2w^2+z^2w^2$, $2x^2z^2 = x^2y^2+x^2w^2$, whence $2x^2z^2-2y^2w^2 = x^2y^2-z^2w^2$. The number $x^2y^2-z^2w^2$ is even, therefore the numbers xy and zw are either both even or both odd. Let $u = xz$, $v = yw$, $r = (xy+zw)/2$, $s = (xy-zw)/2$. Clearly all u, v, r, s are natural numbers. It is easy to check that $u^2-v^2 = 2rs$, $uv = r^2-s^2$. Consequently, $u^4-u^2v^2+v^4 = (r^2+s^2)^2$, which in virtue of theorem 7, implies $u = v$. Since the terms x^2, y^2, z^2, w^2 of the arithmetical progression are supposed to be all different, we may assume that $x < y < z < w$, whence $xz < yw$, i.e. $u < v$, which is a contradiction. Theorem 8 is thus proved. □

13. The equation $x^4+9x^2y^2+27y^4 = z^2$

We present here a proof, due to J. Cel [1], that the above equation is not solvable in natural numbers.

Suppose that the equation

$$x^4+9x^2y^2+27y^4 = z^2 \tag{55}$$

is solvable in positive integers and let x, y, z be a solution in which z takes the least possible value. If $(x, y) = d > 1$ then $x = dx_1$, $y = dy_1$, and by (55) $d^4 \mid z^2$, $d^2 \mid z$, $z = d^2z_1$, x_1, y_1, z_1 being positive integers. Dividing equation (55) throughout by d^4, we get $x_1^4+9x_1^2y_1^2+27y_1^4 = z_1^2$, contrary to the assumption regarding z. Thus $(x, y) = 1$.

If $2 \mid x$ then (55) implies $4 \mid 27y^2-z^2$, hence $2 \mid y$, contrary to $(x, y) = 1$. Thus x is odd. If y were also odd, we would get from (55) $8 \mid z^2-5$ which is impossible. Hence

$$x \text{ is odd, } y \text{ is even.} \tag{56}$$

If $3 \mid x$ then clearly we would have $27 \mid z^2$, whence $9 \mid z$, $81 \mid 27y^4$, $3 \mid y$, contrary to $(x, y) = 1$. We thus have $(x, 3) = 1$.

We also have $(x, z) = 1$. Indeed, denoting (x, z) by d we get from (55) $d \mid 27y^4$. Since $(x, 3y) = 1$ we have $(d, 27y^4) = 1$ hence $d = 1$.

Put $y = 2y_1$. The equation (55) can be written in the following equivalent form

$$27y_1^4 = \left(\frac{z+x^2}{2}+9y_1^2\right)\left(\frac{z-x^2}{2}-9y_1^2\right).$$

The factors on the right-hand side are positive, since their sum and product are positive. Let d_1 be their greatest common divisor. We have $d_1^2 \mid 27y_1^4$, hence by Corollary 2 to Theorem 6a of Chapter I $d_1 \mid 9y_1^2$ and thus $d_1 \mid (x_1^2, z)$. Since $(x, z) = 1$ it follows by the same Theorem 6a that $(x^2, z) = 1$, thus $d_1 = 1$ and by Theorem 8 of Chapter I either

$$\frac{z+x^2}{2}+9y_1^2 = 27a^4, \quad \frac{z-x^2}{2}-9y_1^2 = b^4, \quad y_1 = ab, \tag{57$_1$}$$

or

$$\frac{z+x^2}{2}+9y_1^2 = a^4, \quad \frac{z-x^2}{2}-9y_1^2 = 27b^4, \quad y_1 = ab, \tag{57$_2$}$$

where a, b are coprime positive integers. The system (57_1) is impossible since it gives $x^2+18a^2b^2 = 27a^4-b^4$, $3 \mid b^4+1$. The system (57_2) leads to the equation

$$x^2+18a^2b^2 = a^4-27b^4, \tag{58}$$

which implies that either a or b is even, since by (56) x is odd. If a was even we should get $a^4 = x^2+18a^2b^2+27b^4 = 8k+4$, which is impossible, hence b is even and therefore

$$27b^4 = \left(\frac{a^2+x}{2}-\frac{9}{2}b^2\right)\left(\frac{a^2-x}{2}-\frac{9}{2}b^2\right).$$

Let

$$d_2 = \left(\frac{a^2+x}{2}-\frac{9}{2}b^2, \frac{a^2-x}{2}-\frac{9}{2}b^2\right).$$

We have $d_2^2 \mid 27b^4$, hence $d_2 \mid 9b^2$ and $d_2 \mid x$. It follows that $d_2 \mid (9y^2, x)$ and, since $(3y, x) = 1$, we get $d_2 = 1$. If the numbers $\frac{a^2 \pm x}{2} - \frac{9}{2}b^2$ were both negative we should have $a^2 < 9b^2$ contrary to (58). Thus $\frac{a^2+x}{2} - \frac{9}{2}b^2$, $\frac{a^2-x}{2} - \frac{9}{2}b^2$ are coprime positive integers, and by Theorem 8 of Chapter I

$$\frac{a^2 \pm x}{2} - \frac{9}{2}b^2 = m^4, \qquad \frac{a^2 \mp x}{2} - \frac{9}{2}b^2 = 27n^4, \qquad b = mn,$$

where m, n are positive integers. On addition

$$a^2 = m^4 + 9m^2n^2 + 27n^4$$

and $a \leqslant y_1 < y < z$, which contradicts the initial assumptin about the solution x, y, z. The fact that the equation $x^4 + 9x^2y^2 + 27y^4 = z^2$ has no solution in natural numbers x, y, z is thus proved. □

We note here the existence of two large papers (Lind [1] and Reichardt [1]) devoted to the Diophatine equations $ax^4 + bx^2y^2 + cy^4 = dz^2$.

14. The equation $x^3 + y^3 = 2z^3$

Suppose that this equation has a solution in integers x, y, z such that $x \neq y$ and $z \neq 0$. We may suppose that $(x, y) = 1$, since in the case of $(x, y) = d > 1$ we set $x = dx_1$, $y = dy_1$, whence $d^3 \mid 2z^3$, which implies $d \mid z$ and consequently $z = dz_1$. Therefore $x_1^3 + y_1^3 = 2z_1^3$, where $(x_1, y_1) = 1$.

In virtue of $x^3 + y^3 = 2z^3$, the numbers $x+y$ and $x-y$ are even; so $u = (x+y)/2$ and $v = (x-y)/2$ are integers. Moreover, $x = u+v$, $y = u-v$, and consequently, since $(x, y) = 1$, we have $(u, v) = 1$. We also have $(u+v)^3 + (u-v)^3 = 2z^3$. Hence $u(u^2+3v^2) = z^3$ and, in virtue of $x \neq y$ and $z \neq 0$, we conclude that $uvz = \frac{1}{4}(x^2-y^2)z \neq 0$. If $(u, 3) = 1$, then, by $(u, v) = 1$, we have $(u, u^2+3v^2) = 1$. Moreover, there exist integers z_1 and z_2 such that $u = z_1^3$ and $u^2+3v^2 = z_2^3$. Hence $z_2^3 - z_1^6 = 3v^2$ and consequently $(z_2 - z_1^2)[(z_2 - z_1^2)^2 + 3z_2 z_1^2] = 3v^2$.

We set $t = z_2 - z_1^2$. Then, in virtue of $(z_1, z_2) = 1$, we have $(t, z_1) = 1$ and $t(t^2 + 3tz_1^2 + 3z_1^4) = 3v^2$. It follows that $3 \mid t$; so $t = 3t_1$ and t_1 $(9t_1^2$

$+9t_1 z_1^2+3z_1^4) = v^2$, whence $3 \mid v$; thus $v = 3v_1$ and, in virtue of $(z_1, 3) = 1$, the number $9t_1^2+9t_1 z_1^2+3z_1^4$ is not divisible by 9, whence, by $9 \mid v^2$, we obtain $3 \mid t_1$, and thus $t_1 = 3t_2$. Thus $t_2(27t_2^2+9t_2 z_1^2+z_1^4) = v_1^2$, where, by $(t, z_1) = 1$, we have $(t_2, z_1) = 1$ and $(t_2, 27t_2^2+9t_2z_1^2+z_1^4) = 1$. Moreover, $t_2 = b^2$ and $27b^4+9b^2z_1^2+z_1^4 = c^2$. The numbers b and $|z_1|$ are natural since, if $b = 0$, then also $t_2 = 0$ and, consequently, $t = 0$, whence $z_2 = z_1^2$ and, in virtue of $(z_1, z_2) = 1$, $z_1 = \pm 1$, $z_2 = 1$, which proves that $v = 0$, whence $x = y$, contrary to the assumption regarding x, y, z. On the other hand, if $z_1 = 0$, then $u = 0$, whence $3v^2 = z_2^2$ and consequently $v = 0$, which is impossible. Thus we arrive at the conclusion that the equation $x^4+9x^2y^2+27y^4 = z^2$ is solvable in natural numbers, which, as we know, is impossible.

If $3 \mid u$, then, by $(u, v) = 1$, we have $(v, 3) = 1$, so $u = 3u_1$, whence, in virtue of $u(u^2+3v^2) = z^3$, we have $z = 3z_1$ and $u_1(3u_1^2+v^2) = 3z_1^3$, whence, by $(v, 3) = 1$, we conclude that $3 \mid u_1$. Consequently $u_1 = 3u_2$ and $u_2(27u_2^2+v^2) = z_1^3$. But since $(u_2, v) = 1$ and thus $(u_2, 27u_2^2+v^2) = 1$, we have $u_2 = a^3$, $27u_2^2+v^2 = b^3$, where $(a, b) = 1$ and, in virtue of $(v, 3) = 1$, $(b, 3) = 1$. We then have $27a^6+v^2 = b^3$. Putting $t = b-3a^2$ we obtain $(t, 3) = 1$ and, as can easily be verified, $t(t^2+9a^2t+27a^4) = v^2$. But hence, in virtue of $(a, b) = 1$, we have $(a, t) = 1$. Then by $(t, 3) = 1$, we obtain $(t, t^2+9a^2t+27a^4) = 1$. Consequently, $t = a_1^2$ and $t^2+9a^2t+27a^4 = b_1^2$, whence $a_1^4+9a^2a_1^2+27a^4 = b_1^2$ with $a_1 \neq 0$, $a \neq 0$, because if $a_1 = 0$ then $t = 0$, contrary to $(t, 3) = 1$, and if $a = 0$ then $u = 0$ and consequently $z = 0$, contrary to $z \neq 0$. Thus again we arrive at the conclusion that the equation $x^4+9x^2y^2+27y^4 = z^2$ is solvable in natural numbers, which, as we know, is impossible. This completes the proof due to Antoni Wakulicz [1] of the classical

THEOREM 9. *The equation* $x^3+y^3 = 2z^3$ *has no solution in integers* x, y, z *for which* $x \neq y$ *and* $z \neq 0$.

It follows that *there are no cubes of three different natural numbers which form an arithmetical progression.*

Putting $y = 1$ or $y = -1$, we see that *the equation* $x^3-2z^3 = 1$ *has no solutions in integers* x, z *different from* $x = z = -1$ *and* $x = 1, z = 0$, *and that the equation* $x^3-2z^3 = -1$ *has no solutions in integers* x, z *different from* $x = z = 1$ *and* $x = -1$, $z = 0$.

COROLLARY 1. *There is no triangular number* > 1 *that is the cube of a natural number.*

PROOF. Suppose that there exists a triangular number > 1 which is the cube of a natural number. Then there exist natural numbers $m > 1$ and n such that $m(m+1) = 2n^3$. If m is even, then $m = 2k$, k being a natural number, and $k(2k+1) = n^3$, whence, by $(k, 2k+1) = 1$, we infer that there exist natural numbers x, z such that $k = z^3$, $2k+1 = x^3$, whence $x^3-2z^3 = 1$, which, as we proved above, is impossible. If m is odd, then $m = 2k-1$, where k is a natural number > 1 (since $m > 1$) and $(2k-1)k = n^3$, whence, by $(2k-1, k) = 1$, we infer that there exist natural numbers x, z such that $2k-1 = x^3, k = z^3$. Thus $x^3-2z^3 = -1$, which, in virtue of what we have proved above, is impossible. This completes the proof of Corollary 1. □

COROLLARY 2. *The equation* $x^2-y^3 = 1$ *has no solution in natural numbers apart from* $x = 3$, $y = 2$.

PROOF. Suppose that there exist natural numbers $x \neq 3$ and y such that $x^2-y^3 = 1$. If x were even, then we would have $(x-1, x+1) = 1$ and, in virtue of $(x-1)(x+1) = y^3$, there would exist natural numbers a and b such that $x-1 = a^3$, $x+1 = b^3$, whence $(b-a)(b^2+ab+a^2) = b^3-a^3 = 2$ and, consequently, $b^2+ab+a^2 \mid 2$, which is impossible. Thus x must be odd, and so $x = 2k+1$, where k is a natural number > 1 (for, if $k = 1$, then $x = 3$, contrary to the assumption). Since $x^2-1 = y^3$, the number y must be even, and so $y = 2n$, whence $k(k+1) = 2n^3$, where k is a natural number > 1, contrary to Corollary 1. Thus Corollary 2 has been proved. □

With reference to Corollary 2 we quote the well-known conjecture of Catalan that the only solution of the equation $x^z-y^t = 1$ in natural numbers x, y, z, t each greater than 1 is $x = 3, y = 2, z = 2, t = 3$. The conjecture has not been proved so far, but R. Tijdeman [1] has reduced it to a finite amount of computation, giving an effective bound to the size of possible solutions. The bound has been made explicit by M. Langevin [1], who proved that in every solution $x^z < \exp\exp\exp\exp 730$.

If z and t are primes then, according to J.W.S. Cassels [3] $z \mid y$, $t \mid x$. A. Mąkowski [6] and S. Hyyrö [1] deduced from this that there are no three consecutive natural numbers such that each of them is a non--trivial power of a natural number. It is, however, easy to prove that there are no four consecutive natural numbers of this kind; in fact, among any four consecutive natural numbers there is a number which divided by 4 yields the remainder 2, and so it cannot be a non-trivial power of an even natural number. We note here S.S. Pillai's conjecture that if $u_1, u_2, \ldots$ is an infinite sequence of natural numbers which are consecutive natural numbers, each of them being a power of a natural number with exponent greater than 1, then $\lim\limits_{n\to\infty} (u_{n+1} - u_n) = +\infty$ (Pillai [8]). This conjecture is clearly equivalent to the following one: for each natural number m the number of all the systems x, y, z, t of natural numbers, each greater than 1, satisfying the equation $x^y - z^t = m$ is finite. It seems interesting to know for which natural number m there exist natural numbers x, y, z, t greater than 1, satisfying the above equation. It is easy to prove that, in fact, this property applies to every natural number which is not of the form $4k+2$, where $k = 0, 1, 2, \ldots$ In this connection one can ask whether for every natural number n there exists a natural number m such that the equation $x^y - z^t = m$ has at least n different solutions in natural numbers x, y, z, t, each being greater than 1. The answer to this question is positive. For, if $k = 1, 2, \ldots, n$, and $m = 2^{2n}$, then

$$m = 2^{2n} = (2^{2n-k-1} + 2^{k-1})^2 - (2^{2n-k-1} - 2^{k-1})^2.$$

We also have

$$3^{2^n} - 2^{2^n} = (3^{2^{n-k}})^{2^k} - (2^{2^{n-k}})^{2^k} \quad \text{for} \quad k = 1, 2, \ldots, n.$$

In the sequence u_n mentioned above the terms that are less than or equal to 400 are the following: 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343, 361, 400.

The corresponding terms of the sequence $u_{n+1} - u_n$ are 3, 4, 1, 7, 9, 2, 5, 4, 13, 15, 17, 19, 21, 4, 3, 16, 25, 27, 20, 9, 18, 13, 33, 35, 19, 18, 39.

COROLLARY 2^{a}. *The equation* $x^2 - y^3 = 1$ *has no solutions in rational numbers apart from the following ones:* $x = 0$, $y = 1$, $x = \pm 1$, $y = 0$, $x = \pm 3$, $y = 2$.

PROOF. Suppose that rational numbers x, y satisfy the equation $x^2 - y^3 = 1$. Let $x = h/g$, $y = r/s$, where g, s are natural numbers and h, r are integers such that $(h, g) = (r, s) = 1$. Since $x^2 - y^3 = 1$, we have $h^2s^3 - g^2r^3 = g^2s^3$. Hence $h^2s^3 = g^2(r^3 + s^3)$. Consequently, by $(g, h) = 1$, we have $g^2 \mid s^3$. On the other hand, $g^2r^3 = (h^2 - g^2)s^3$, whence, in virtue of $(r, s) = 1$, we obtain $s^3 \mid g^2$. From this we infer that $g^2 = s^3$. Consequently, for a natural number m we have $g = m^3$, $s = m^2$, whence $h^2 - r^3 = m^6$. Therefore $r^3 = (h + m^3)(h - m^3)$, where $(m, h) = 1$.

If one of the numbers h and m is even and the other is odd, then $(h+m^3, h-m^3) = 1$ and, consequently, there exist integers a and b such that $h+m^3 = a^3$, $h-m^3 = b^3$, whence $a^3+(-b)^3 = 2m^3$. But, since $m \neq 0$ in virtue of what has been proved above, we must have $a = -b$, whence $h = 0$ and, consequently, $x = 0$, $y = 1$.

If both m and h are odd, then $\left(\frac{h+m^3}{2}, \frac{h-m^3}{2}\right) = 1$ and $2|r$, so $r = 2r_1$ and $2r_1^3 = \left(\frac{h+m^3}{2}\right)\left(\frac{h-m^3}{2}\right)$. Consequently, there exist integers a and b such that $h \pm m^3 = 4a^3$, $h \mp m^3 = 2b^3$. Hence $b^3+(\pm m)^3 = 2a^3$. If $a = 0$, then $h = \mp m^3 = \mp g$, whence $x = \mp 1$, $y = 0$. If $a \neq 0$, then, as we know, b must be equal to $\pm m = a$. Therefore $h = 4a^3 \mp m^3 = \pm 3m^3 = \pm 3g$, whence $x = \pm 3$, $y = 2$.

Thus Corollary 2^a is proved. □

COROLLARY 3. *If n is a natural number greater than* 1, *then the number* $1^3+2^3+\ldots+n^3$ *is not the cube of a natural number.*

PROOF. As we know $1^3+2^3+\ldots+n^3 = \left(\frac{n(n+1)}{2}\right)^2 = t_n^2$. If the number t_n^2 were the cube of a natural number, then also t_n would be the cube of a natural number, contrary to Corollary 1.

To see this it is sufficient to recall the theorem of the preceding chapter (corollary to Theorem 16) which states that, if natural numbers a, b, l, m satisfy the conditions $(l, m) = 1$, $a^l = b^m$, then there exists a natural number n such that $a = n^m$ and $b = n^l$. □

It is much more difficult to prove that for $n > 1$ the number $1^2+2^2+\ldots+n^2$ is the square of a natural number only in the case where $n = 24$ (¹).

A somewhat related problem, whether the equation $1^n+2^n+\ldots+(m-1)^n = m^n$ has a solution in natural numbers m, $n > 1$, is not yet solved. P. Erdős conjectures that the answer is negative. L. Moser [2] has proved that this is indeed the case for $m \leqslant 10^{10^6}$ (cf. Best and te Riele [1]).

(¹) This problem was formulated by E. Lucas [1]. The first solution based on the theory of elliptic functions was given by G. N. Watson [1]. The solution based on the theory of number fields was given by Ljunggren [5]. See also Trost [1].

Lastly we note that it can be proved that the equation $x^3+y^3=z^3$ has no solutions in integers $x, y, z \neq 0$. It follows that the number 1 is not the sum of the cubes of two non-zero rational numbers (cf. Chapter XI, § 10).

15. The equation $x^3+y^3=az^3$ with $a>2$

THEOREM 10. *If a is a natural number greater than 2 and is not divisible by the cube of any natural number greater than 1 and if the equation*

$$x^3+y^3=az^3 \tag{59}$$

has a solution in integers x, y, z with $(x, y)=1$, $z \neq 0$, then it has infinitely many such solutions (cf. Nagell [5], p. 246).

PROOF. Suppose that integers x, y, z, $(x, y)=1$, $z \neq 0$, satisfy equation (59). We have $(x, z)=1$; for, putting $d=(x, z)$, we have $d^3 \mid az^3-x^3=y^3$, whence $d \mid y$, which, in virtue of $(x, y)=1$, proves that $d=1$. Similarly $(y, z)=1$. Let

$$\delta=\left(x(x^3+2y^3), -y(2x^3+y^3), z(x^3-y^3)\right). \tag{60}$$

We have

$$x(x^3+2y^3)=\delta x_1, \tag{61}$$

$$-y(2x^3+y^3)=\delta y_1, \tag{62}$$

$$z(x^3-y^3)=\delta z_1, \tag{63}$$

where x_1, y_1, z_1, are integers and $(x_1, y_1, z_1)=1$. In virtue of the identity

$$\left(x(x^3+2y^3)\right)^3-\left(y(2x^3+y^3)\right)^3=(x^3+y^3)(x^3-y^3)^3,$$

from (59) we infer that the numbers x_1, y_1, z_1 satisfy the equation $x_1^3+y_1^3=az_1^3$.

If $x=y$, then, by $(x, y)=1$ we have $x=y=\pm 1$, and, consequently, by (59), $az^3=\pm 2$, which is impossible, since $a>2$. Thus $x \neq y$, which by (63) proves that $z_1 \neq 0$.

If $d=(x_1, y_1)$, then $d^3 \mid x_1^3+y_1^3=az_1^3$. If $d>1$ and $(d, z_1)=1$, then we would have $(d^3, z_1^3)=1$, and, consequently, since $d^3 \mid az_1^3$, we would obtain $d^3 \mid a$, contrary to the assumption that a is not divisible by the cube of any natural number greater than 1. Thus either $d=1$ or $d>1$ and $(d, z_1)>1$, whence $(x_1, y_1, z_1)>1$, which is impossible.

Hence we conclude that $d=1$, and so $(x_1, y_1)=1$, and further, since $x_1^3+y_1^3=az_1^3$, we see that also $(x_1, z_1)=1$. Since $(x, y)=1$, we have

$(x, y^4) = 1$ and, in virtue of (62), $(\delta y_1, x) = 1$ (for, if $d_1 \mid \delta y_1$ and $d_1 \mid x$, then, by (62), $d_1 \mid y^4$) and *a fortiori*, $(\delta, x) = 1$. Similarly, in virtue of (61), we have $(\delta x_1, y) = 1$, whence $(\delta, y) = 1$. Since $(x, z) = (y, z) = 1$, we have $(xy^3, z) = 1$. If $d \mid \delta$ and $d \mid z$, then by (59) and (61) we have $d \mid x^3+y^3 \mid x^4+xy^3$ and $d \mid x^4+2yx^3$, whence $d \mid xy^3$. Consequently, in virtue of $d \mid z$ and $(xy^3, z) = 1$, we have $d = 1$, i.e. $(\delta, z) = 1$. Hence $(\delta, x) = (\delta, y) = (\delta, z) = 1$, and by (61), (62), (63) we conclude that δ is a divisor of each of the numbers x^3+2y^3, $2x^3+y^3$, x^3-y^3, and so it is a divisor of the number $x^3+2y^3+2(x^3-y^3) = 3x^3$. Therefore, since $(\delta, x) = 1$, we see that $\delta \mid 3$. Thus $\delta = 1$ or $\delta = 3$, and so in any case we have $\delta \leqslant 3$. If $x = 0$, then, by $(x, y) = 1$, we have $y = \pm 1$, contrary to (59) since $a > 2$. Similarly we find that also $y \neq 0$. Each of the numbers x and y is then different from zero and, since also $x \neq y$, we have $|x-y| \geqslant 1$. If x, y are both positive or both negative, then $x^2+xy+y^2 = (x-y)^2+3xy \geqslant 1+3xy \geqslant 4$ and $|x^3-y^3| = |x-y|\,|(x-y)^2+3xy| \geqslant 4$. If one of the numbers x, y is positive and the other negative, then $xy < 0$ and $x^2-xy+y^2 = (x+y)^2-3xy \geqslant 4$; for, clearly, $x+y \neq 0$, since otherwise $x = -y$, which by (59) and $a > 2$ would imply $z = 0$, contrary to the assumption. Thus in any case $|x^3-y^3| \geqslant 4$. Since $\delta \leqslant 3$, formula (63) implies $|z_1| > |z|$. This shows that, if the number a satisfies the conditions of the theorem, then from each solution of equation (59) in integers x, y, z with $(x, y) = 1$ and $z \neq 0$ we obtain another solution of the equation in integers x_1, y_1, z_1 with $(x_1, y_1) = 1$ and $|z_1| > |z|$, which proves that there are infinitely many such solutions. Theorem 10 is thus proved. □

The equations

$$x^3+y^3 = 3z^3, \qquad x^3+y^3 = 4z^3, \qquad x^3+y^3 = 5z^3$$

are insolvable in integers x, y, z with $z \neq 0$ (cf. Selmer [1], [2]).

On the other hand, it follows from Theorem 10 that each of the equations

$$x^3+y^3 = 6z^3, \qquad x^3+y^3 = 7z^3, \qquad x^3+y^3 = 9z^3$$

has infinitely many solutions in integers x, y, z with $(x, y) = 1$ and $z \neq 0$. In fact, we use Theorem 10 and note that the numbers 17, 37, 21 satisfy the first equation, the numbers 2, -1, 1 satisfy the second one, and the numbers 2, 1, 1 the third one (cf. Nagell [5], pp. 247–248). From this we will deduce some corollaries in Chapter XI § 9.

16. Triangular numbers

As we know from § 4 the number $t_n = n(n+1)/2$ is called the nth triangular number. The list of the first 20000 triangular numbers was published in 1762 by E. de Joncourt [1]. K. Zarankiewicz [1] has noticed that all the numbers 21, 2211, 222111,... are triangular.

We have

$$21 = \frac{6\cdot 7}{2}, \quad 2211 = \frac{66\cdot 67}{2}, \quad 222111 = \frac{666\cdot 667}{2}, \ldots$$

We leave the simple proof of this fact to the reader.

The following examples of similar sequences are due to T. Józefiak [1]:

55, 5050, 500500, 50005000, ...

5151, 501501, 50015001, 5000150001, ...

78, 8778, 887778, 88877778, ...

45, 4950, 499500, 49995000, ...

45, 2415, 224115, 22241115, ...

It is easy to prove that there exist infinitely many pairs of triangular numbers such that the sum of the numbers of each pair is a triangular number. In fact, it is easy to check that for natural numbers k we have $t_{k-1}+k = t_k$ (where $t_0 = 0$). Hence, for $k = t_n$ $(n = 1, 2, \ldots)$, we obtain $t_{t_n-1}+t_n = t_{t_n}$. In particular, $t_2+t_2 = t_3$, $t_5+t_3 = t_6$, $t_9+t_4 = t_{10}$, $t_{14}+t_5 = t_{15}$. As found by M. N. Khatri [1], it is easy to verify that also $t_{3k}+t_{4k+1} = t_{5k+1}$, $t_{5k+4}+t_{12k+9} = t_{13k+10}$, $t_{8k+4}+t_{15k+9} = t_{17k+10}$ for $k = 0, 1, 2 \ldots$ In particular, $t_6+t_9 = t_{11}$, $t_9+t_{13} = t_{16}$, $t_9+t_{21} = t_{23}$, $t_{12}+t_{24} = t_{27}$. We also have $t_{4k^2+5k+2} = t_{4k^2+5k}+t_{4k+2}$ for $k = 1, 2, \ldots$

We prove even more: there exist infinitely many pairs of natural numbers x, y that satisfy the system of equations

$$(64)\qquad t_x+t_{2y} = t_{3y} \quad\text{and}\quad t_x-t_{2y} = t_{y-1}.$$

It is easy to prove that each of the two equations of (64) is equivalent to the equation

$$(65)\qquad x^2+x = 5y^2+y.$$

Consequently, it is sufficient to prove that equation (65) has infinitely many solutions in natural numbers x, y. By the identity

$$(161x+360y+116)^2+161x+360y+116-5(72x+161y+52)^2-$$
$$-(72x+161y+52) = x^2+x-5y^2-y$$

it follows that, if numbers x, y form a solution of equation (65) in natural numbers, then the numbers $u = 161x+360y+116$ and $v = 72x+161y+52$ are solutions of (65) in natural numbers u, v greater than x, y, respectively. Since the numbers $x = 2$ and $y = 1$ satisfy equation (65), this shows that (65) has infinitely many solutions in natural numbers x, y (cf. Sierpiński [32]). J. Browkin [1], using the results of P. F. Teilhet [1], has presented a method for finding all the pairs of triangular numbers such that the sum and the difference of the numbers of each pair are triangular numbers. For $x \leqslant 100$ these are the pairs t_x, t_y with $(x, y) = (6, 5), (18, 16), (37, 27), (44, 39), (86, 65), (91, 54)$.

As we already know (compare I, § 4) there exist infinitely many triangular numbers which are squares.

It is worth noticing that, as has been known since Euler, for each natural n the number $\frac{(3+2\sqrt{2})^n-(3-2\sqrt{2})^n}{4\sqrt{2}}$ is a natural number and its square is a triangular number (cf. Sierpiński [30]).

On the other hand, it has been proved by W. Ljunggren [4] that there are only two triangular numbers whose squares are also triangular, namely t_1 and t_6.

We now prove

THEOREM 11. *There is no triangular number* > 1 *which is the fourth power of a natural number.*

PROOF. Suppose to the contrary that, for some natural numbers m and $n > 1$, the equality $\frac{1}{2}n(n+1) = m^4$ holds. Then also $n(n+1) = 2m^4$. Suppose that n is an even number, and so $n = 2k$ and, consequently, $k(2k+1) = m^4$. Since $(k, k+1) = 1$, there exist natural numbers x, y such that $k = y^4$, $2k+1 = x^4$, whence $2y^4+1 = x^4$. If n is odd, then $n = 2k-1$ and, consequently, $(2k-1)k = m^4$. This, in virtue of $(2k-1, k) = 1$, implies the existence of natural numbers x, y such that $2k-1 = x^4$, $k = y^4$. From this we infer that $2y^4-1 = x^4$ and, since $2k-1 = n > 1$, we have $y > 1$. Hence $y^4 = k > 1$.

Thus all that remains to complete the proof is to show that

1) there are no natural numbers x, y such that $2y^4+1 = x^4$,

2) there are no natural numbers x and $y > 1$ such that $2y^4-1 = x^4$.

In order to prove 1) we note that if $2y^4+1 = x^4$, then we have $(y^2)^4+x^4 = (y^4+1)^2$, contrary to Corollary 2 of § 6. To prove 2) we suppose that $2y^4-1 = x^4$, whence $(y^2)^4-x^4 = (y^4-1)^2$. But since $y^4 > 1$, y^4-1

is a natural number, contrary to Corollary 1 of § 6. Theorem 11 is thus proved. □

However, it may happen that for rational numbers t and u, $\frac{1}{2}t(t+1) = u^4$, for instance, for $t = \frac{32}{49}$, we have $\frac{1}{2}t(t+1) = (\frac{6}{7})^4$.

We note here that the equation $2y^4+1 = z^2$ is insolvable in natural numbers y, z, but $2 \cdot 13^4 - 1^4 = 239^2$.

It can be proved that the equation $2y^4-1 = z^2$ has only two solutions in natural numbers y, z, namely $y = z = 1$ and $y = 13$, $z = 239$ (Ljunggren [1]).

It can be deduced from the well-known results about the equation $x^n + y^n = 2z^n$ (Dénes [1]) that a triangular number cannot be the nth power of a natural number, where $2 < n \leqslant 30$.

On the other hand, by a general theorem (Schinzel and Tijdeman [1]) an equation $P(x) = y^m$, where P is a polynomial with rational coefficients and with at least two distinct zeros, can have only finitely many solutions in integers x, y with $y > 1$, $m > 2$. Hence a triangular number cannot be the nth power of a natural number for n greater than a suitable n_0. According to E. Z. Chein [2] one can take $n_0 = 7.877 \cdot 10^8$.

It is easy to see that for a natural number n the number $n(n+1)$ cannot be the square of a natural number. In fact, if it were, i.e. if $n(n+1) = a^2$, (a being a natural number) then, by $(n, n+1) = 1$, the numbers n and $n+1$ would be squares. Hence $n = k^2$, $n+1 = l^2$, whence $(l-k)(l+k) = l^2-k^2 = 1$, which is impossible. For $n = \frac{1}{3}$, however, we have $\frac{1}{3}(\frac{1}{3}+1) = (\frac{2}{3})^2$.

The proof that *the product of two consecutive numbers cannot be a power with exponent greater than* 1 *of a natural number* is analogous.

The proof of a theorem of Chr. Goldbach stating that the product of any three consecutive natural numbers cannot be the square of a natural number is also easy.

In fact, we easily prove a theorem which is even slightly more general, namely that *the product of any three consecutive natural numbers cannot be a power with exponent greater than* 1 *of a natural number*. In fact, suppose that for natural numbers n, k and $s > 1$ we have $n(n+1)(n+2) = k^s$. Since $(n+1, n(n+2)) = 1$, in virtue of Theorem 8 of Chapter I there exist natural numbers a, b such that $n+1 = a^s$ and $n(n+2) = b^s$. Consequently, $1 = (n+1)^2 - n(n+2) = (a^2)^s - b^s$, which is impossible.

As proved by P. Erdős and J. L. Selfridge [1], the product of k consecutive positive integers, where $k > 1$, cannot be a power with exponent greater than 1 of a natural number neither can the product of k consecutive odd natural numbers, where $k > 1$, be a power with exponent > 1 of a natural number (Erdös [5]).

We note here that for natural numbers $k > 3$ and $n \geqslant 2k$ the number $\binom{n}{k}$ canot be a power with the exponent greater than 1 of a natural number, as was proved by P. Erdös [11].

A number of the form $T_n = \frac{1}{6}n(n+1)(n+2)$, where n is a natural number, is called a *tetrahedral number*. The name refers to the number of spheres of the same radius which can be packed together in a teatrahedron.

The first ten tetrahedral numbers are the following 1, 4, 10, 20, 35, 56, 84, 120, 165, 220. For $n = 1, 2, 48$ we obtain the tetrahedral numbers 1^2, 2^2, 140^2, which are squares. It can be proved that these are the only tetrahedral numbers with this property.

This theorem results, as has been proved by A. Meyl [1], from the fact that the number $s_n = 1^2+2^2+ \ldots +n^2$ is a square only in the case where either $n = 1$ or $n = 24$ (cf. § 14). Conversely, suppose that for a natural number n we have $s_n = m^2$, where m is a natural number. Then, as we can easily verify, $4s_n = T_{2n}$. Consequently we have $T_{2n} = (2m)^2$. Thus, by the assertion regarding tetrahedral numbers which are squares, we infer that $2n$ must be equal to 2 or 48, and so $n = 1$, or $n = 24$, as required.

There exist natural numbers which are both tetrahedral and triangular. As proved by E. T. Avanesov [1], the only numbers of this kind are the numbers $n = 1, 10, 120, 1540, 7140$. For these numbers we have $n = \frac{1}{2}x(x+1) = \frac{1}{6}y(y+1)(y+2)$ with $x = 1, 4, 15, 55, 119$; $y = 1, 3, 8, 20, 34$, respectively.

It is easy to prove that $T_n - T_{n-1} = t_n$ and $T_n + T_{n+1} = 1^2+2^2+ \ldots +(n+1)^2$

It can be proved that *there exist infinitely many pairs of tetrahedral numbers such that the sum (or the difference) of the numbers of each pair is a tetrahedral number* (Röhr [1], Sierpiński [33], Wunderlich [1], cf. Bremner [1]). I do not know whether there is any pair of tetrahedral numbers such that both the sum and the difference of the numbers of the pair are tetrahedral numbers. H. E. Salzer [1] has conjectured that every square is the sum of at most four tetrahedral numbers. He has verified this for the squares $\leqslant 10^6$. In particular $1^2 = T_1$, $2^2 = T_2$, $3^2 = T_1+T_2+T_2$, $4^2 = T_1+T_1+T_2+T_3$, $5^2 = T_1+T_2+T_4 = T_1+T_2+T_3+T_3$, 6^2

$= T_1 + T_5$, $7^2 = T_2 + T_3 + T_5$, $8^2 = T_2 + T_2 + T_6$, $9^2 = T_1 + T_2 + T_4 + T_6$, $10^2 = T_2 + T_4 + T_4 + T_6$.

It is easy to prove that every natural number is the algebraic sum of four tetrahedral numbers. In fact, we have $1 = T_1 + T_4 - T_3 - T_3$, $2 = T_4 - T_3 - T_2 - T_2$, and for natural numbers n greater than 2 we have $n = T_n + T_{n-2} - T_{n-1} - T_{n-1}$.

It is more difficult to prove that each natural number is the sum of at most eight tetrahedral numbers (Watson [2]).

The natural numbers $\leqslant 10^7$ are the sums of at most five tetrahedral numbers (Salzer and Levine [1]).

17. The equation $x^2 - Dy^2 = 1$

In this section we consider the equation

$$x^2 - Dy^2 = 1 \tag{66}$$

and its solutions in integers, provided D is a natural number. Equation (66) is called alternatively the *Fermat equation* or the *Pell equation*, though the latter had nothing to do with it.

Apart from the trivial solutions $x = 1$, $y = 0$ and $x = -1$ and $y = 0$, the solutions of equation (66) in integers x, y, both different from zero, can be arranged in classes of four solutions in each such that any two solutions of the same class differ in the signs at the x's and y's respectively. Clearly, in every class there exists exactly one solution in natural numbers. These we call simply *natural solutions*. It is clear that in order to find all the solution of equation (66) in integers it suffices to find its natural solutions.

The case where D is the square of a natural number is of no interest. In fact, equation (66) can then be written in the form

$$(x - ny)(x + ny) = 1,$$

whence $x + ny \mid 1$, which is impossible since x, y are natural numbers. We conclude that

If D is the square of a natural number, then equation (66) *is not solvable in natural numbers x, y.*

In order to show that if D is not the square of a natural number then equation (66) does have solutions in natural numbers, we prove the following

LEMMA. *If a natural number D is not the square of a natural number, then there exist infinitely many different pairs of integers x, y satisfying the inequalities*

$$(67)\qquad y \neq 0 \quad \textit{and} \quad |x^2-Dy^2| < 2\sqrt{D}+1.$$

PROOF. Let n denote a natural number. For each of the numbers $k = 0, 1, 2, \ldots, n$ we denote by l_k the greatest natural number $\leqslant k\sqrt{D}+1$. We then have

$$l_k \leqslant k\sqrt{D}+1 \quad \text{and} \quad l_k+1 > k\sqrt{D}+1.$$

Hence

$$(68)\qquad 0 < l_k-k\sqrt{D} \leqslant 1.$$

$n+1$ numbers $l_k-k\sqrt{D}$ $(k = 0, 1, 2, \ldots, n)$ are all different, since if $l_k-k\sqrt{D} = l_{k'}-k'\sqrt{D}$, then we would have $l_k-l_{k'} = (k-k')\sqrt{D}$, which for $k \neq k'$ is impossible; for, otherwise $\sqrt{D}$ would be a rational number and consequently D would be the square of a rational number and therefore, by Theorem 8 of Chapter I, it would be the square of a natural number, contrary to the assumption.

In virtue of (68), each of the numbers $u = l_k-k\sqrt{D}$ $(k = 0, 1, 2, \ldots, n)$ must satisfy one of the inequalities:

$$0 < u \leqslant \frac{1}{n}, \quad \frac{1}{n} < u \leqslant \frac{2}{n}, \quad \ldots, \quad \frac{n-1}{n} < u \leqslant \frac{n}{n}.$$

It follows that at least two different values u' and u'' satisfy the same inequality, i.e.

$$\frac{j-1}{n} < u' \leqslant \frac{j}{n}, \quad \frac{j-1}{n} < u'' \leqslant \frac{j}{n},$$

where j is one of the numbers $1, 2, \ldots, n$. Since by assumption $u' \neq u''$, we may assume that, for instance, $u' > u''$. The inequalities $u' \leqslant k/n$ and $u'' > (k-1)/n$ imply together that

$$0 < u'-u'' < \frac{1}{n}.$$

Since $u' = l_k-k\sqrt{D}$, $u'' = l_i-i\sqrt{D}$, where k, i are taken from the sequence $0, 1, 2, \ldots, n$, then, putting $x = l_k-l_i$, $y = i-k$, we obtain

$$(68^a)\qquad 0 < x-y\sqrt{D} < \frac{1}{n}.$$

Obviously, x, y are integers and $y = i-k$. Hence y, as the difference of two different terms of the sequence 0, 1, 2, ..., n, is different from zero and the modulus of y is not greater than n, i.e.

$$0 < |y| \leqslant n. \tag{69}$$

In virtue of (68^a) we have

$$y\sqrt{D} < x < y\sqrt{D} + \frac{1}{n}.$$

Since, by (69), $-n \leqslant y \leqslant n$, we have

$$-\left(n\sqrt{D} + \frac{1}{n}\right) < -n\sqrt{D} < x < n\sqrt{D} + \frac{1}{n},$$

and consequently

$$|x| < n\sqrt{D} + \frac{1}{n}.$$

Hence, by (69),

$$|x+y\sqrt{D}| \leqslant |x| + |y|\sqrt{D} < 2n\sqrt{D} + \frac{1}{n}.$$

This multiplied by the number $|x-y\sqrt{D}|$ which is less than $1/n$ (cf. (68^a)) gives

$$|x^2 - Dy^2| < 2\sqrt{D} + 1.$$

Thus we have proved that for each natural number n there exists a pair of integers x, y satisfying inequalities (67) and (68^a).

Using this fact we now prove that there exist infinitely many pairs of integers x, y satisfying inequalities (67) and

$$0 < x - y\sqrt{D}. \tag{70}$$

Suppose, on the contrary, that there are only finitely many such pairs and let

$$(x_1, y_1), \quad (x_2, y_2), \quad \ldots, \quad (x_s, y_s) \tag{71}$$

be all of them. Plainly each of the numbers

$$x_1 - y_1\sqrt{D}, \quad x_2 - y_2\sqrt{D}, \quad \ldots, \quad x_s - y_s\sqrt{D} \tag{72}$$

is positive. Let α denote the least of them. Further, let n be a natural number such that

$$\frac{1}{n} < \alpha. \tag{73}$$

In virtue of what we have proved before there exists at least one pair of integers x, y satisfying inequalities (67) and (68^a). By (68^a) and (73) we have $0 < x - y\sqrt{D} < \alpha$. But since α is the least among the numbers of (72), then the number $x - y\sqrt{D}$ cannot be any of them, which means that the pair (x, y) is different from all the pairs (71) and also satisfies inequalities (67) and (68^a) and hence inequality (70). This contradicts the definition of pairs (71), and proves that there are infinitely many pairs of integers x, y satisfying (67) and (70) and hence, *a fortiori*, inequalities (67). This concludes the proof of the lemma. ☐

THEOREM 12. *If a natural number D is not the square of a natural number, then the equation $x^2 - Dy^2 = 1$ has infinitely many solutions in natural numbers x, y.*

PROOF. Since the number of integres whose moduli are less than $2\sqrt{D} + 1$ is finite and, by the lemma, there are infinitely many pairs (x, y) satisfying inequalities (67), then there are infinitely many pairs of integers x, y for which $x^2 - Dy^2$ is equal to a fixed number k, obviously different from zero, since the case $D = x^2/y^2$ is excluded. Denote by Z the set of all such pairs x, y.

For an integer t, denote by $r(t)$ the remainder obtained by dividing the number t by k. For x, y both running over the set Z, we consider the pairs $r(x)$, $r(y)$. Clearly, there are at most k^2 different ones among them.

We now divide the set Z into classes, putting two pairs x, y and x', y' into the same class if $r(x) = r(x')$ and $r(y) = r(y')$. In virtue of what we have said above, the number of different pairs $r(x)$, $r(y)$ is finite, and so, since Z is infinite, at least one of the classes is infinite. In that class then there exist two pairs a, b and c, d for which at least one of the equalities $|a| = |c|$, $|b| = |d|$ fails, because for a given pair a, b there are at most four pairs c, d for which both equalities hold.

Each of the differences $a^2 - Db^2$ and $c^2 - Dd^2$ is equal to k (since both a, b and c, d belong to the set Z). But since, moreover, a, b and c, d belong to the same class, we see that $r(a) = r(c)$ and $r(b) = r(d)$. Therefore, there exist integers t and v such that $a - c = kt$ and $b - d = kv$. Consequently,

$$a = c + kt, \qquad b = d + kv, \tag{74}$$

where t and v are integers. Multiplying the equalities

$$a^2 - Db^2 = k, \qquad c^2 - Dd^2 = k \tag{75}$$

and applying the identity

$$(a^2-Db^2)(c^2-Dd^2) = (ac-Dbd)^2-D(ad-cb)^2$$

we obtain

$$(ac-Dbd)^2-D(ad-cb)^2 = k^2. \tag{76}$$

In virtue of (74) and (75) we have

$$ac-Dbd = (c+kt)c-D(d+kv)d = c^2-Dd^2+k(ct-Ddv)$$
$$= k(1+ct-Dvd)$$

and also

$$ad-cb = (c+kt)d-c(d+kv) = k(dt-cv).$$

Therefore, if we divide equation (76) by k^2 throughout, we obtain

$$(1+ct-Ddv)^2-D(dt-cv)^2 = 1,$$

from which, putting

$$x = |1+ct-Ddv|, \qquad y = |dt-cv|,$$

we derive the equality

$$x^2-Dy^2 = 1.$$

We are now going to prove that $y \neq 0$. If $y = 0$ we would have $|x| = 1$, so

$$1+ct-Ddv = \pm 1, \qquad dt-cv = 0.$$

Now, multiplying the first of these equalities by c and the second by $-Dd$ and then adding them up, we would have

$$c+(c^2-Dd^2)t = \pm c,$$

whence, in virtue of formulae (74) and (75), we would obtain $a = \pm c$, i.e. $|a| = |c|$. Similarly, multiplying the first of the equalities by d, the second by $-c$ and then adding them up, we would have

$$d+(c^2-Dd^2)v = \pm d,$$

whence, by (75) and (74), we would obtain $b = \pm d$, i.e. $|b| = |d|$. But this and the equality $|a| = |c|$ obtained above contradict the definition of the pairs a, b and c, d.

Thus we have proved the existence of at least one pair x, y of integers such that $x^2-Dy^2 = 1$ and $y \neq 0$ (which clearly shows that also $x \neq 0$). Changing, if necessary, the signs of the integers x and y, we obtain a natural solution of equation (66).

If the equality $x^2-Dy^2 = 1$ holds for natural numbers x, y then, clearly, $(2x^2-1)^2-D(2xy)^2 = 1$ with $2xy > y$. Thus from any solution of equation (66) in natural numbers x, y we derive another solution of (66) in natural numbers x', y' with $x' > x$ and $y' > y$. This proves that equation (66) has infinitely many solutions in natural numbers.

Theorem 12 is thus proved. □

In order to find effectively a solution of equation (66) we may apply the following procedure: In $1+Dy^2$ we substitute successively for y the natural numbers 1, 2, 3, ... and denote by u the first y for which $1+Dy^2$ is the square of a natural number. Then we set $1+Du^2 = t^2$. We assert that the pair (t, u) is the solution of equation (66) for which t, u are the least natural numbers. In fact, for any other solution of equation (66) in natural numbers x, y we have $y > u$ and, consequently, $x = \sqrt{1+Dy^2} > \sqrt{1+Du^2} = t$, whence also $x > t$.

In some particular cases it is very easy to find the least solution of equation (66). This is for instance the case when D is of the form a^2-1, where a is a natural number (> 1). (It is easy to see that then the least solution of (66) in natural numbers is $t = a, u = 1$.) Similarly, this is also the case when $D = a(a+1)$, where a is a natural number. Then the least solution is $t = 2a+1, u = 2$. Namely we have $(2a+1)^2-D\cdot 2^2 = 1$, and, on the other hand, if for a natural number x, $x^2-D\cdot 1^2 = 1$, then we would have $x^2 = a^2+a+1$, whence $x^2 > a^2$, so $x > a$; consequently, $x \geqslant a+1$, and therefore $x^2 \geqslant a^2+2a+1 > a^2+a+1$, which is a contradiction. It is more difficult to prove that if $D = a^2+2$, where a is a natural number, then the least solution of (66) in natural numbers is $t = a^2+1$, $u = a$; and also if $D = a^2+1$, then $t = 2a^2+1$, $u = 2a$.

EXAMPLES. 1. For $D = 2$ equation (66) assumes the form $x^2-2y^2 = 1$. Substituting 1 and 2 for y in $1+2y^2$ successively, we obtain the numbers 2 and 9 respectively, the latter being square. Therefore the least solution is here $x = 3$, $y = 2$.

2. For $D = 3$ equation (66) becomes $x^2-3y^2 = 1$. Substituting 1 for y in $1+3y^2$, we obtain a square (of the number 2). Thus the least solution is here $t = 2$, $u = 1$.

3. For $D = 5$, i.e. for the equation $x^2-5y^2 = 1$, one has to substitute 1, 2, 3, 4 for y in $1+5y^2$ successively in order to obtain the values 6, 21, 46, 81, the last of which is a square. Consequently the least solution is here $t = 9$, $u = 4$.

4. For $D = 11$, i.e. for the equation $x^2-11y^2 = 1$, we substitute 1, 2, 3 for y in $1+11y^2$ successively and obtain the values 12, 45, 100 respectively. Consequently the least solution is here $t = 10$, $u = 3$.

Although the above method of finding the least solution of equation (66) is very simple, it cannot be regarded as useful in practice. In fact, for some comparatively small numbers it requires a large number of trials.

E.g. in order to find the least solution of the equation $x^2-13y^2 = 1$ in natural numbers, which are $t = 649$, $u = 180$, one needs 180 trials. A very striking example of this kind is the equation

$$x^2-991y^2 = 1 \tag{77}$$

whose least solution in natural numbers is

$$t = 379516400906811930638014896080,$$

$$u = 12055735790331359447442538767.$$

This is very instructive example, showing that it is (sometimes) impossible to deduce the general theorem even from a very long sequence of trials. Substituting $1, 2, 3, \ldots, 10^{28}$ for y in equation (77) we do not obtain a solution, though the conclusion drawn from this, namely that equation (77) is insolvable in natural numbers, is false.

In Chapter VIII, § 5, we present another, more convenient, method of finding the least solution of equation (66) in natural numbers; it gives the least solution of equation (77) without long calculations.

With regard to Theorem 12 we note here that for D which is not the square of a natural number (and hence not the square of a rational number) one can easily find all the solutions of equation (66) in rational numbers x, y. In point of fact, for an arbitrary rational number r we put $x = (r^2+D)/(r^2-D)$, $y = 2r/(r^2-D)$, then

$$1+Dy^2 = 1+D\left(\frac{2r}{r^2-D}\right)^2 = \frac{(r^2-D)^2+4Dr^2}{(r^2-D)^2} = \left(\frac{r^2+D}{r^2-D}\right)^2 = x^2,$$

and so $x^2-Dy^2 = 1$. It is easy to prove that all the solutions of equation (66) in rational numbers can be obtained in this way.

The task of finding all the solutions of equation (66) in rational numbers x, y is equivalent to that of finding the solutions of the equation $x^2-Dy^2 = z^2$ in integers x, y, z.

We now turn to the problem of finding all the solutions of equation (66) in natural numbers.

THEOREM 13. *All the solutions of the equation $x^2-Dy^2 = 1$ in natural numbers are contained in the infinite sequence*

$$(t_0, u_0), \quad (t_1, u_1), \quad (t_2, u_2), \quad \ldots, \tag{78}$$

where (t_0, u_0) is the least natural solution and (t_k, u_k) are defined inductively by the formulae

$$t_{k+1} = t_0 t_k + Du_0 u_k, \qquad u_{k+1} = u_0 t_k + t_0 u_k, \qquad k = 0, 1, 2, \ldots \tag{79}$$

PROOF. To see that the numbers of sequence (78) indeed satisfy equation (66) we note that (t_0, u_0) does satisfy (66) and, if for an integer $k \geqslant 0$ the pair (t_k, u_k) satisfies (66), then numbers (79) are natural and, in virtue of the equality

$$\begin{aligned} t_{k+1}^2 - Du_{k+1}^2 &= (t_0 t_k + Du_0 u_k)^2 - D(u_0 t_k + t_0 u_k)^2 \\ &= (t_0^2 - Du_0^2)(t_k^2 - Du_k^2), \end{aligned}$$

also the pair (t_{k+1}, u_{k+1}) satisfies equation (66).

Thus all that remains in order to complete the proof is to show that every solution (x, y) of the equation $x^2-Dy^2 = 1$ is contained in sequence (78). To this end we prove the following

LEMMA. *If (x, y) is a solution of the equation $x^2-Dy^2 = 1$ in natural numbers such that $u_0 < y$, then for*

$$(80) \qquad \xi = t_0 x - Du_0 y, \qquad \eta = -u_0 x + t_0 y$$

ξ, η are both natural numbers, $\eta < y$ and $\xi^2 - D\eta^2 = 1$.

PROOF OF THE LEMMA. In virtue of (80) we have

$$\xi^2 - D\eta^2 = (t_0 x - Du_0 y)^2 - D(-u_0 x + t_0 y)^2 = (t_0^2 - Du_0^2)(x^2 - Dy^2),$$

and consequently, by $t_0^2 - Du_0^2 = 1$ and $x^2-Dy^2 = 1$, we find $\xi^2 - D\eta^2 = 1$.

Therefore it is enough to show that, if ξ and η are natural numbers and $\eta < y$, then the inequalities

$$0 < t_0 x - Du_0 y \quad \text{and} \quad 0 < -u_0 x + t_0 y < y$$

hold. In order to do this we note first that

$$D^2u_0^2 y^2 = (t_0^2 - 1)(x^2 - 1) < t_0^2 x^2, \quad \text{whence} \quad Du_0 y < t_0 x,$$

and that, since $u_0 < y$, we have

$$\left(\frac{x}{y}\right)^2 = D + \frac{1}{y^2} < D + \frac{1}{u_0^2} = \left(\frac{t_0}{u_0}\right)^2.$$

Consequently $x/y < t_0/u_0$, which implies $u_0 x < t_0 y$, whence $0 < -u_0 x + t_0 y$.

To verify the inequality $-u_0 x + t_0 y < y$ we note that, in virtue of $t_0^2 = Du_0^2 + 1$, we have $t_0 > 1$, whence $x^2(2-2t_0) < 0 < (t_0 - 1)^2$. Then adding $x^2(t_0^2 - 1)$ to each side of the last inequality we obtain $x^2(t_0^2 - 2t_0 + 1) < x^2(t_0^2 - 1) + (t_0 - 1)^2$, whence $(x^2 - 1)(t_0 - 1)^2 < x^2(t_0^2 - 1)$, and consequently $Dy^2(t_0-1)^2 < x^2Du_0^2$ whence $y^2(t_0-1)^2 < x^2u_0^2$; therefore $y(t_0-1) < xu_0$, that is $-xu_0+t_0y < y$, as required. The lemma is thus proved. ☐

Now suppose that there exist solutions of the equation $x^2-Dy^2 = 1$ in natural numbers which are not contained in sequence (78). Among them there exists a solution (x, y) for which y takes the least possible value. However, y must be still greater than u_0, since the solution (t_0, u_0) is the least solution and consequently the equality $y = u_0$ implies $x = t_0$, contrary to the assumption that (x, y) does not belong to sequence (78). In virtue of the lemma, taking for ξ, η the numbers of the form (80) defined with the aid of the solution x, y, we see that they satisfy the equation $x^2-Dy^2 = 1$ and $\eta < y$. It follows from the definition of the solution (x, y) that the solution (ξ, η) belongs to sequence (78). Therefore for some integer $k \geqslant 0$ we have $\xi = t_k$, $\eta = u_k$. Then, by formulae (79) and (80) and the fact that $t_0^2-Du_0^2 = 1$, we obtain

$$t_{k+1} = t_0\xi+Du_0\eta = t_0(t_0x-Du_0y)+Du_0(-u_0x+t_0y) = (t_0^2-Du_0^2)x = x,$$

$$u_{k+1} = u_0\xi+t_0\eta = u_0(t_0x-Du_0y)+t_0(-u_0x+t_0y) = (t_0^2-Du_0^2)y = y,$$

which proves that (x, y) is one of the solutions of sequence (78), contrary to the assumption. Thus the assumption that there exists a solution of the equation $x^2-Dy^2 = 1$ which does not belong to sequence (78) leads to a contradiction. This completes the proof of Theorem 13. ☐

In particular, for the equation $x^2-2y^2 = 1$, where $t_0 = 3$, $u_0 = 2$, by formulae (79) we find that each of the remaining solutions of the equation belongs to the sequence $t_1 = 3^2+2\cdot 2^2 = 17$, $u_1 = 2\cdot 3+3\cdot 2 = 12$, $t_2 = 99$, $u_2 = 70$, $t_3 = 577$, $u_3 = 408, \ldots$

As has been observed by Antoni Wakulicz, formulae (79) imply the following equalities:

$$t_{k+1} = 2t_0t_k-t_{k-1}, \quad u_{k+1} = 2t_0u_k-u_{k-1} \quad \text{for} \quad k = 1, 2, \ldots$$

Now we are going to prove that

$$t_{n-1}+u_{n-1}\sqrt{D} = (t_0+u_0\sqrt{D})^n \quad \text{for} \quad n = 1, 2, \ldots \tag{81}$$

Formula (81) is trivial for $n=1$. Suppose it is true for a natural number n. Applying (79) with $k=n-1$, we find that

$$\begin{aligned} t_n+u_n\sqrt{D} &= t_0 t_{n-1}+Du_0 u_{n-1}+(u_0 t_{n-1}+t_0 u_{n-1})\sqrt{D} \\ &= (t_0+u_0\sqrt{D})(t_{n-1}+u_{n-1}\sqrt{D}), \end{aligned}$$

whence, by (81), we obtain

$$t_n+u_n\sqrt{D} = (t_0+u_0\sqrt{D})^{n+1},$$

which proves formula (81) for $n+1$, and hence, by induction, for an arbitrary natural number.

Thus, Theorem 13 and formula (81) imply the following theorem:

THEOREM 14. *If t_0, u_0 is the least solution of the equation $x^2-Dy^2=1$ in natural numbers, then in order that a pair of natural numbers t, u be a solution of this equation it is necessary and sufficient for the equality*

$$t+u\sqrt{D} = (t_0+u_0\sqrt{D})^n \tag{82}$$

to hold for a natural number n.

For arbitrary natural numbers a, b, c, d the equality $a+b\sqrt{D}=c+d\sqrt{D}$ implies $a=c$, $b=d$ (because the number $\sqrt{D}$ is irrational). Therefore, expanding the right-hand side of equality (81) according to the binomial formula and then reducing it to the form $c+d\sqrt{D}$, where c, d are natural numbers, we obtain $t_{n-1}=c$, $u_{n-1}=d$.

We note that from formula (82), which gives all the solutions of equation (66) in natural numbers, we can easily obtain a formula giving all the solutions of this equation in integers.

In fact, if t, u is a solution of equation (66) in natural numbers, then in virtue of Theorem 14 equality (82) holds for a suitable natural number n. But this, in virtue of an easily verifiable equality

$$t-u\sqrt{D} = 1/(t+u\sqrt{D})$$

(for the proof we observe that $t^2-Du^2=1$) implies

$$t-u\sqrt{D} = (t_0+u_0\sqrt{D})^{-n}.$$

The numbers t, $-u$ are obtained from the numbers t, u by a simple change of sign and the remaining two solutions belonging to the same class are $(-t, -u)$, $(-t, u)$.

This leads us to the following

THEOREM 15. *Every solution of equation* (66) *in integers t, u is obtained from the formula*

$$t+u\sqrt{D} = \pm(t_0+u_0\sqrt{D})^k,$$

where k is a suitably chosen integer, and u_0, t_0 denote the least solution in natural numbers. Conversely, every pair of integers t, u obtained from the above formula is a solution of equation (66).

It is worth-while to note that even the solution $t = \pm 1$, $u = 0$ is obtained from this formula, namely for $k = 0$.

The solutions of equation (66) supply us with a method of approximating the square root of a natural number by rational numbers. In fact, it follows from (66) that

$$x-y\sqrt{D} = 1/(x+y\sqrt{D}),$$

whence

$$0 < x/y-\sqrt{D} = 1/y(x+y\sqrt{D}) < 1/y^2\sqrt{D} < 1/y^2.$$

Therefore, *if x, y is a solution of equation* (66) *in natural numbers x, y, then the fraction x/y approximates the* (*irrational*) *number $\sqrt{D}$ with a better accuracy than the reciprocal of the square of the denominator.* (It follows immediately from equation (66) that x/y is an irreducible fraction.)

In particular, the fourth of the listed solutions of the equation $x^2-2y^2 = 1$ in natural numbers yields the fraction 577/408, which approximates the number $\sqrt{2}$ with an accuracy to five decimal places (since $408^2 > 10^5$).

In order to obtain a better accuracy in a smaller number of steps we use the following formulae, which enable us to pass from the solutions t_{n-1}, u_{n-1} to the solution t_{2n-1}, u_{2n-1} immediately. In virtue of (81) one has

$$t_{2n-1}+u_{2n-1}\sqrt{D} = (t_0+u_0\sqrt{D})^{2n} = (t_{n-1}+u_{n-1}\sqrt{D})^2,$$

whence, since $t_{n-1}^2-Du_{n-1}^2 = 1$, one obtains

$$t_{2n-1} = t_{n-1}^2+Du_{n-1}^2 = t_{n-1}^2+(t_{n-1}^2-1) = 2t_{n-1}^2-1,$$

$$u_{2n-1} = 2t_{n-1}u_{n-1}.$$

Thus we pass from the fraction t_{n-1}/u_{n-1} to the fraction

$$t_{2n-1}/u_{2n-1} = (2t_{n-1}^2-1)/(2t_{n-1}u_{n-1}).$$

In particular, from the fraction $t_2/u_2 = 99/70$, which is an approximation of number $\sqrt{2}$, we pass to the fraction $t_5/u_5 = 19601/13860$, which approximates $\sqrt{2}$ with an accuracy of eight decimal places. With regard to number $\sqrt{2}$ we note here that in 1950 R. Coustal found its decimal expansion with 1033 digits (1), and in 1951 H. S. Uhler presented the decimal expansion of this number with 1543 digits (2).

Returning to the equation $x^2 - 2y^2 = 1$ we prove that it has no solution in natural numbers x, y for which x is the square of a natural number. In fact, if there were a solution x, y, with $x = u^2$, then u would be an odd number greater than 1. Consequently $u^2 = 8k+1$, where k would be a natural number. Further, in virtue of the identity $(u^2-1)(u^2+1) = u^4 - 1 = 2y^2$, we would have $8k(4k+1) = y^2$, which by $(2k, 4k+1) = 1$ would imply $2k = a^2$, a being a natural number. Therefore $u^2 - 1 = 8k = (2a)^2$, which is impossible, since two consecutive numbers cannot be squares of natural numbers. It follows that *the equation* $x^4 - 2y^4 = 1$ *is insolvable in natural numbers* x, y.

It is easy to prove that also *the equation* $v^4 - 2u^2 = -1$ *is insolvable in natural numbers* u, v *different from* $u = v = 1$.

To see this we note that, if $u > 1$ and v satisfy the equation $v^4 - 2u^2 = -1$, then we would have $u^4 - v^4 = (u^2-1)^2$, where $u, v, d^2 - 1$ would be natural numbers. But this contradicts Corollary 1 of Theorem 3, § 6, p. 52.

It can be proved, however, that each of the equations

$$x^4 - 2y^4 = z^2, \qquad u^4 - 2v^4 = -w^2$$

has infinitely many solutions in natural numbers. In particular, (3, 2, 7) and (113, 84, 7967) are solutions of the first equation, (1, 13, 239) and (1343, 1525, 2165017) are solutions of the second one.

Most Diophantine equations of second degree with two unknowns can be reduced to the equation of Pell (cf. Skolem [2], p. 46). For instance, this is the case with the equation

$$(x+1)^3 - x^3 = y^2. \tag{83}$$

In fact one sees that equation (83) is equivalent to the equation $(2y)^2 - 3(2x+1)^2 = 1$. Consequently, in order to solve equation (83) in integers it is sufficient to find the solution of the equation $u^2-3v^2 = 1$ in integers u, v such that u is even and v is odd. Apart from the trivial solution $u = 1$, $v = 0$, all the other integer solutions are defined by the natural numbers u, v satisfying our equation. Since the least solution in natural numbers u, v is $u_0 = 2$, $v_0 = 1$, according to Theorem 13 all the natural solutions are contained in the infinite sequence (u_k, v_k), $k = 0, 1, 2, \ldots$, where

---

(1) Cf. Coustal [1]. Compare also the remarks of E. Borel [2] concerning this expansion.

(2) Cf. Uhler [1]; ibidem the decimal expansion with 1301 digits of the number $\sqrt{3}$ can be found. Now $\sqrt{2}$ has been computed to 10^6 digits (cf. Dutka [1]) and $\sqrt{3}$ to 24576 digits (Beyer, Metropolis and Neugerard [1]).

$$u_{k+1} = 2u_k+3v_k \quad \text{and} \quad v_{k+1} = u_k+2v_k, \quad k = 0, 1, 2, \ldots$$

It follows that, if u_k is even and v_k is odd, then u_{k+1} is odd and v_{k+1} is even; conversely, if u_k is odd and v_k is even, then u_{k+1} is even and v_{k+1} is odd. From this we easily conclude that all the solutions of the equation $u^2-3v^2 = 1$ in natural numbers u, v with u even and v odd are (u_{2k}, v_{2k}) where $k = 0, 1, 2, \ldots$

It can also be easily proved (but this we leave to the reader) that all the solutions of equation (83) in natural numbers x, y are contained in the infinite sequence (x_k, y_k), $k = 1, 2, \ldots$, where $x_0 = 0$ $y_0 = 1$, and $x_k = 7x_{k-1}+4y_{k-1}+3$, $y_k = 12x_{k-1}+7y_{k-1}+6$, $k = 1, 2, \ldots$

It has been proved that, if natural numbers x, y satisfy equation (83), then the number y is the sum of the squares of two consecutive natural numbers. In particular, we have $8^3-7^3 = (2^2+3^2)^2$, $105^3-104^3 = (9^2+10^2)^2$.

As noticed by A. Rotkiewicz [3] the problem of solving the equation

$$(u-v)^5 = u^3-v^3 \tag{84}$$

in natural numbers u, v with $u > v$ reduces to that of solving equation (83) in natural numbers x, y.

To prove this we observe that, on the one hand, if natural numbers x, y satisfy equation (83), then, putting $u = y(x+1)$, $v = yx$, we obtain $u-v = y$ and $u^3-v^3 = y^3[(x+1)^3-x^3] = y^5 = (u-v)^5$, i.e. formula (84). On the other hand, if natural numbers u, v with $v < u$ satisfy equation (84), then, denoting $y = (u, v)$, $x = v/y$, $t = u/y$, we have $(x, t) = 1$ and, in virtue of $u > v$, $t > x$. Therefore, by (84), we have $y^5(t-x)^5 = y^3(t^3-x^3)$, whence $y^2(t-x)^4 = (t^3-x^3)/(t-x)$, which, in virtue of the identity $(t^3-x^3)/(t-x) = (t-x)^2+3tx$, proves that $(t-x)^2 \mid 3tx$. Hence, since $(t, x) = 1$, we obtain $t-x = 1$, and consequently $t = x+1$, $u = y(x+1)$ and $y^2 = (x+1)^3-x^3$, which gives equality (83). Thus all the solutions of equation (84) in natural number u, v with $u > v$ are obtained from the solutions of equation (83) by putting $u = y(x+1)$, $v = yx$.

18. The equations $x^2+k=y^3$, where k is an integer

These equations have long been investigated by many authors.

We start with a number of general theorems, which can be applied to the equations with various values for k (cf. Mordell [1]).

THEOREM 16. *If a is an odd integer and b an even integer not divisible by* 3 *and having no common divisor of the form* $4t+3$ *with a and, lastly, if* $k=b^2-a^3$ *and k is not of the form* $8t-1$, *then the equation* $x^2+k=y^3$ *has no solutions in integers x, y.*

PROOF. Suppose to the contrary that x, y are integers such that $x^2+k=y^3$. Since b is even and a is odd, the number $k=b^2-a^3$ is odd. Then, if y were even, then x would be odd and consequently $8\mid x^2-1$, $8\mid y^3$, whence, since $k+1=y^3-(x^2-1)$, we would have $8\mid k+1$, contrary to the assumption that k is not of the form $8t-1$. Therefore y must be odd, and consequently x is even. So $x=2u$ and, since $b=2c$, we have $x^2+b^2=4(u^2+c^2)=y^3+a^3=(y+a)(y^2-ay+a^2)$. Since $y-a$ is even and a is odd, $y^2-ay+a^2=(y-a)y+a^2$ is odd. Consequently $4\mid y+a$ and $y+a=4v$. Hence $y-a=4v-2a$, $y=4v-a$ and $(y-a)y=4w+2a^2$; therefore $y^2-ay+a^2=4w+3a^2$. Since a is odd, the right-hand side of the last equality must be of the form $4t+3$.

Consequently (¹), it has a prime divisor p of the same form, such that the maximal exponent s for which p^s divides the number $4w+3a^2$ is an odd number. Let $s=2\alpha-1$. Therefore, since $p^{2\alpha-1}\mid y^2-ay+a^2$ and $y^2-ay+a^2\mid x^2+b^2$, we have $p^{2\alpha-1}\mid x^2+b^2$. Let $d=(x,b)$, $x=dx_1$, $b=db_1$. Then $(x_1,b_1)=1$ and $p^{2\alpha-1}\mid d^2(x_1^2+b_1^2)$. Since, as we know and as can be found in Chapter XI, the sum of the squares of two numbers such that at least one of them is not divisible by a prime p of the form $4t+3$ cannot be divisible by p, we have $p^{2\alpha-1}\mid d^2$, whence $p^{2\alpha}\mid d^2$ and $p^\alpha\mid d$. Consequently $p^\alpha\mid x$ and $p^\alpha\mid b$, whence $p^{2\alpha}\mid(y+a)(y^2-ay+a^2)$. Therefore, since the maximal exponent s for which $s^s\mid y^2-ay+a^2$ is odd, we have $p\mid y+a$. Since also $p\mid y^2-ay+a^2=(y+a)(y-2a)+3a^2$, we find $p\mid 3a^2$, which, in virtue of $p\mid b$ and the fact that b is not divisible by 3, implies $p\mid a$, contrary to the assumption regarding a and b. Theorem 16 is thus proved. □

(¹) The argument is to be found in Chapter V, p. 218

COROLLARY. *The equation* $x^2+k = y^3$ *has no solution in integers* x, y *for* $k = 3, 5, 17, -11, -13$, *since* $3 = 2^2-1^3, 5 = 2^2-(-1)^3, -11 = 4^2-3^3$, $17 = 4^2-(-1)^3$, $-13 = 70^2-17^3$.

THEOREM 17. *If* a *is an integer of the form* $4t+2$ *and* b *an odd integer not divisible by* 3 *and having no common divisor of the form* $4t+3$ *with* a, *and if* $k = b^2-a^3$, *then the equation* $x^2+k = y^3$ *has no solution in integers* x, y.

PROOF. Suppose to the contrary that x, y are integers such that $x^2+k = y^3$. Since $k = b^2-a^3$ and in virtue of the assumptions on a and b, we see that the number k is of the form $8t+1$. Consequently, if y were an even integer, then $x^2 = y^3-k$ would be of the form $8t-1$, which is impossible. Thus y must be odd and hence x is even. If y were of the form $4t+1$, then $y+a$ would be of the form $4t+3$ and would also have a prime divisor p of this form such that the exponent μ of p in the factorization into prime numbers of $y+a$ would be odd, i.e. $\mu = 2\alpha-1$. Further, since $x^2+b^2 = y^3+a^3$, we would have $p^{2\alpha-1} \mid x^2+b^2$, whence, as in the proof of theorem 16, we would conclude that $p^\alpha \mid b$ and $p^\alpha \mid x$ and hence that $p \mid 3a^2$. But since $p \mid b$ and b is not divisible by 3, we have $p \neq 3$; this would imply that $p \mid a$, contrary to the assumption regarding the numbers a and b. Thus all that remains to be considered is the case where y is of the form $4t+3$. Then $y-a$ is of the form $4t+1$ and $y(y-a)$ is of the form $4t+3$. Therefore y^2-ay+a^2 is of the form $4t+3$, whence, in analogy to the proof of Theorem 16, we infer that the number $x^2+b^2 = y^3+a^3 = (y+a)(y^2-ay+a^2)$ has a prime divisor p of the form $4t+3$ the exponent of which in the factorization into prime numbers is odd. But this, as we have seen, leads to a contradiction. The proof of Theorem 17 is thus completed. ☐

COROLLARY. *The equation* $x^2+k = y^3$ *has no solution in integers* x, y *for* $k = 9$ *and* $k = -7$, *since* $9 = 1^2-(-2)^3$ *and* $-7 = 1^2-2^3$ (¹).

THEOREM 18. *The equation* $x^2+12 = y^3$ *has no solution in integers* x, y.

PROOF. Suppose to the contrary that integers x, y satisfy the equation $x^2+12 = y^3$. If the number x is even, then $x = 2x_1$ and the number y is also even, and so $y = 2y_1$. Hence $x_1^2+3 = 2y_1^3$ and x_1 is an odd number;

(¹) The proof for $k = -7$ was found by V. A. Lebesgue [2] in 1869.

consequently x_1^2 is of the form $8t+1$, and therefore $2y_1^3 = x_1^2+3$ is of the form $8t+4$, whence y_1^3 is of the form $4t+2$. But this is impossible, since the cube of an even number is divisible by 8. From this we conclude that x and hence y must be odd. We have

$$x^2+4 = y^2-8 = (y-2)(y^2+2y+4).$$

Since y is odd, the number y^2+2y+4 must be of the form $4t+3$. Therefore the number x^2+2^2, where $(x, 2) = 1$, has a divisor of the form $4k+3$, which, as we know, is impossible. Thus the assumption that the equation $x^2+12 = y^3$ is solvable in integers leads to a contradiction, and this proves Theorem 18. ☐

We note here that, as has been proved by Mordell, a more general theorem holds: If $k = (2a)^2-(2b)^3$, where a is an odd integer not divisible by 3 and b is an integer of the form $4t+3$ and moreover (a, b) has no divisor of the form $4t+3$, then the equation $x^2+k = y^3$ has no solutions in integers x, y.

In particular, since $12 = 2^2-(-2)^3$, $-20 = 14^2-6^3$, the last assertion implies that the equation $x^2+k = y^3$ has no solutions in integers x, y for $k = 12$, $k = -20$.

THEOREM 19. *The equation* $x^2+16 = y^3$ *has no solution in integers* x, y.

PROOF. If x were even, then y would also be even, and so $x = 2x_1$, $y = 2y_1$, x_1 and y_1 being integers. Hence $x_1^2+4 = 2y_1^3$, and consequently x_1 would be even, and so $x_1 = 2x_2$, whence $2x_2^2+2 = y_1^3$. Therefore $y_1 = 2y_2$, whence $x_2^2+1 = 4y_2^3$, which is impossible. Thus x must be odd, and consequently y^3 is of the form $8t+1$. But this implies that y is also of the form $8t+1$; consequently $y-2$ is of the form $8t-1$. Since $y-2 \mid y^3-8 = x^2+8$, the number x^2+8 has a divisor of the form $8t-1$. It follows that x^2+8 has a prime divisor p either of the form $8k+5$ or of the form $8k+7$. Therefore $p \mid x^2+8$, which is known to be untrue for prime p either of the form $8k+5$ or of the form $8k+7$ (1). Theorem 19 is thus proved. ☐

THEOREM 20. *The equation* $x^2-16 = y^3$ *has no solution in integers different from* $x = \pm 4$, $y = 0$.

---

(1) This will be shown in Chapter IX, p. 345.

PROOF. Suppose that integers x, y satisfy the equation $x^2-16 = y^3$. If the number x were odd, then we would have $(x+4, x-4) = 1$, and hence, since $(x+4)(x-4) = y^3$, there would exist odd integers a, b such that $x+4 = a^3$, $x-4 = b^3$, whence $a^3-b^3 = 8$; but this is impossible, since the number 8 has no representation as the difference of the cubes of odd integers, which is easy to see. Therefore x must be even. Hence $x = 2x_1$, which implies that y is also even; consequently $y = 2y_1$. Hence $x_1^2-4 = 2y_1^3$, which proves that x_1 is even, and so $x_1 = 2x_2$. It follows that also y_1 must be even, and so $y_1 = 2y_2$; consequently $x_2^2-1 = 4y_2^3$. The last equality implies that x_2 is odd, and so $x_2 = 2x_3+1$. Hence $4x_3^2+4x_3 = 4y_2^3$ and therefore $x_3(x_3+1) = y_2^3$, which, in virtue of $(x_3, x_3+1) = 1$, implies that there are integers a and b such that $x_3 = a^3$, $x_3+1 = b^3$. But two consecutive integers are the cubes of integers only in the case where they are either -1 and 0, or 0 and 1, respectively. From this we conclude that $y_2^3 = 0$, whence $y_2 = 0$ and $y = 0$ and consequently $x = \pm 4$. Theorem 20 has thus been proved. □

A. Thue [2] (cf. Mordell [2]) has proved that for every integer $k \neq 0$ the equation $x^2+k = y^3$ has finitely many solutions in integers. Corollary 2 to Theorem 9 furnishes a complete solution of the equation $x^2-1 = y^3$. The equation $x^2+1 = y^3$ has no solution in integers $x, y \neq 0$ and, more generally, in rationals $x, y \neq 0$. The equation $x^2+2 = y^3$ has a unique solution in positive integers $x = 5$, $y = 3$. Although this fact has been known since Fermat (¹) its proof is difficult. It is to be found in Uspensky and Heaslet [1]. The proof presented there does not require the theory of the field $Q(\sqrt{-2})$. It is still more difficult to prove that the equation $x^2-2 = y^3$ has no solutions in integers except $x = 1, y = -1$. The first proof found by A. Brauer [1] in 1926 was based on the theory of ideals; the proof given in Uspensky and Heaslet [1] avoids it.

The number of integral solutions of the equation $x^2+k = y^3$ can be arbitrarily large. It was proved by T. Nagell [3] in 1930 that there exist for $k = -17$ precisely 16 solutions. These are $(x, y) = (\pm 3, -2)$, $(\pm 4, -1)$, $(\pm 5, 2)$, $(\pm 9, 4)$, $(\pm 23, 8)$, $(\pm 282, 43)$, $(\pm 375, 52)$, $(\pm 378661, 5234)$.

To the equation $x^2+k = y^3$, O. Hemer has devoted his thesis (Hemer [1]). Some corrections of it as well as additional information are to be found in his subsequent note (Hemer [2]) and in the book of London and

---

(¹) Fermat [1], pp. 345 and 434. The first rigorous proof was given by T. Pépin [1]. The proof by Euler can be made rigorous.

Finkelstein [1]. Hemer has found all the solutions of the equation $x^2+k = y^3$ in integers x, y for all k with $-100 \leqslant k < 0$.

For positive $k \leqslant 100$ the same has been done by F. B. Coghlan and N. M. Stephens [1]. In theory but not in practice the problem is solved for every k by the following inequality of A. Baker [1]:

$$|x^3-y^2| > 10^{-10}(\log|x|)^{10^{-4}} \quad \text{if} \quad x^3 \neq y^2$$

for all integers x, y (see also Stark [2]).

It has been conjectured by M. Hall, Jr. [3] that for a suitable $c > 0$ the inequality

$$0 < |x^3-y^2| < c\sqrt{|x|}$$

has no integer solutions and it has been recently proved by Danilov [1] that for infinitely many integers x, y

$$0 < |x^3-y^2| < 0.97\sqrt{|x|}$$

Danilov's idea gives in fact a stronger theorem, namely

THEOREM 21. *For infinitely many positive integers x, y we have the inequality*

$$0 < x^3-y^2 < \frac{54}{25}\sqrt{\frac{x}{5}}.$$

PROOF. We have the identity

$$(t^2+6t-11)^3-(t^2-5)^2[(t+9)^2+4] = 1728t-3456.$$

In virtue of Theorem 14 with $\xi_0 = 930249$, $\eta_0 = 83204$, n odd the equation $\xi^2-125\eta^2 = 1$ has infinitely many solutions in positive integers ξ, η with $125 | \xi+1$. Setting

$$t = 1364\xi+15250\eta-9, \qquad u = 61\xi+682\eta,$$

we find t odd, $125|t-2$,

$$(t+9)^2+4 = 500u^2,$$

$$\left(\frac{t^2+6t-11}{20}\right)^3-\left(\frac{(t^2-5)}{4}u\right)^2 = \frac{27}{125}(t-2).$$

Now, taking

$$x = \frac{t^2+6t-11}{20}, \qquad y = \frac{(t^2-5)}{4}u,$$

we get $t = \sqrt{20x+20}-3 < \sqrt{20x}$, $0 < t-2 < \sqrt{20x}$ and the theorem follows. □

The equation $x^2+k = y^3$, where $2 < |k| \leqslant 20$, is solvable in integers $x, y \neq 0$ for $k = 4, 7, 11, 13, 15, 18, 19, 20, -3, -5, -8, -9, -10, -12, -15, -17, -18, -19$; since $2^2+4 = 2^3$, $1^2+7 = 2^3$, $4^2+11 = 3^3$ (also $58^2+11 = 15^3$), $70^2+13 = 17^3$, $7^2+15 = 4^3$, $3^2+18 = 3^3$, $18^2+19 = 7^3$, $14^2+20 = 6^3$, $2^2-3 = 1^3$, $2^2-5 = (-1)^3$, $4^2-8 = 2^3$, $1^2-9 = (-2)^3$, $3^2-10 = (-1)^3$, $2^2-12 = (-2)^3$, $4^2-15 = 1^3$ (also $1138^2-15 = 109^3$), $4^2-17 = (-1)^3$ (also $3^2-17 = (-2)^3$, $19^2-18 = 7^3$, $12^2-19 = 5^3$. For all the other k, where $2 < |k| \leqslant 20$, the equation is insolvable even in rational numbers $x, y \neq 0$; except that for $k = -11$ there is no solution in integers but there are rational solutions, e.g.

$$\left(\frac{19}{8}\right)^2 - 11 = \left(\frac{7}{4}\right)^3 .$$

By the identity

$$\left(\frac{27y^6-36x^2y^3+8x^4}{8x^3}\right)^2 + y^3 - x^2 = \left(\frac{9y^4-8x^2y}{4x^2}\right)^3$$

every solution of the equation $x^2+k = y^3$ in rational numbers $x, y \neq 0$ yields another solution, and, in fact, it has been proved by R. Fueter [1] that, if there is one such solution, then for $k \neq -1{,}432$ there are infinitely many.

It is worth-while to note that the solutions of the equation $x^2+k = y^3$ in rational numbers are obtained from the solutions of the equation $u^2+kw^6 = v^3$ in integers u, v and $w \neq 0$ by putting $x = u/w^3$, $y = v/w^2$. In fact, it is easy to verify that then $x^2+k = y^3$; on the other hand, suppose that x, y are two arbitrary rational numbers satisfying the equation $x^2+k = y^3$. Let $x = m/n$, $y = r/s$, where m, r are integers and n, s natural numbers. Then, putting $u = mn^2s^3$, $v = rn^2s$, $w = ns$, we see that the numbers u, v, w are integers, $w \neq 0$; they satisfy the equation $u^2+kw^6 = v^3$ and $u/w^3 = m/n$, $v/w^2 = r/s$.

The solutions of the equation $x^2+k = y^3$ in rational numbers have been investigated by J. W. S. Cassels [1], [2] and E. S. Selmer [3]. J. W. S. Cassels [1] has presented the so-called basic solutions of the equation $u^2+kw^6 = v^3$ in integers u, v, w for all values of k absolutely $\leqslant 50$ for which non-trivial solutions exist (on page 268), as well as a long list of references to literature (pages 271–273). Selmer has given a continuation of Cassels' table for $|k|$ between 50 and 100.

We note here that the theorem stating that the equation $u^3+v^3 = w^3$ has no solutions in integers u, v, w, with $uvw = 0$ is equivalent to the theorem stating that the equation $x^2+432 = y^3$ is insolvable in rational numbers x, y other that $x = \pm 36$, $y = 12$.

The argument for this purpose proceeds as follows. Suppose that rational numbers x, y satisfy the equation $x^2+432 = y^3$, $x \neq \pm 36$. Obviously we must have $y > 0$. Numbers $x/36$ and $y/12$ are rational, $y/12 > 0$, and, after reducing them to the same denominator, we get $x/36 = k/n$, $y/12 = m/n$, where k is an integer and m, n are natural numbers. Without loss of generality we may assume that each of the numbers k and n is divisible by 2, since we can replace n, k, m by $2n$, $2k$, $2m$ respectively, if necessary. We set $u = \dfrac{n+k}{2}$, $v = \dfrac{n-k}{2}$, $w = m$. Plainly, u, v, w are integers and, moreover, $w > 0$. We have $u^3+v^3-w^3 = \left(\dfrac{n+k}{2}\right)^3 + \left(\dfrac{n-k}{2}\right)^3 - m^3 = \dfrac{n^3}{4} + \dfrac{3nk^2}{4} - m^3$. But $k = \dfrac{nx}{36}$, $m = \dfrac{ny}{12}$; therefore $u^3+v^3-w^3 = \dfrac{n^3}{4} + \dfrac{3n^3x^2}{4\cdot 36^2} - \dfrac{n^3y^3}{12^3} = \dfrac{n^3}{1728}(432+x^2-y^3) = 0$. This leads us to the conclusion that if the equation $x^2+432 = y^3$ has a solution in rational numbers x, y and $x \neq \pm 36$, then the equation $u^3+v^3 = w^3$ is solvable in integers u, v, w with $uvw \neq 0$. On the other hand, suppose that integers u, v, w with $uvw \neq 0$ satisfy the equation $u^3+v^3 = w^3$. Since $u^3+v^3 = (u+v)(u^2-uv+v^2)$ and $w \neq 0$, we have $u+v \neq 0$. Therefore, putting $x = 36(u-v)/(u+v)$, $y = 12w/(u+v)$, we get rational numbers x, y such that

$$y^3-x^2 = \frac{12^3(u^3+v^3)}{(u+v)^3} - \frac{36^2(u-v)^2}{(u+v)^2}$$

$$= \frac{12^3(u^2-uv+v^2)-36^2(u^2-2uv+v^2)}{(u+v)^2} = 432.$$

Consequently $x^2+432 = y^3$. We have thus proved that the equation $u^3+v^3 = w^3$ has a solution in integers u, v, w with $uvw \neq 0$ if and only if the equation $x^2+432 = y^2$ is solvable in rational numbers x, y, where $x \neq \pm 36$. It can be proved similarly (cf. Cassels [1], p. 243) that the equation $u^3+v^3 = Aw^3$, where A is a natural number, is solvable in integers u, v, w with $w \neq 0$ if and only if the equation $x^2+432A^2 = y^3$ is solvable in rational numbers x, y.

In order to prove that the equation $x^3+y^3 = z^3$ is insolvable in integers $\neq 0$ it suffices to show that the equation $x^2-16 = y^3$ has no solutions in rational numbers x, y different from zero. To see this we simply observe that if integers u, v, w different from zero satisfied the equation $u^3+v^3 = w^3$, then the rational numbers $x = 4(v^3+w^3)/u^3$ and $y = 4vw/2$ would both be different from zero and would satisfy the equation $x^2-16 = y^3$.

We note that, as shown by T. R. Bendz [1], the theorem called *Fermat Last Theorem*, which states that the equation $x^n+y^n = z^n$ is insolvable in positive integers x, y, z for $n > 2$, is equivalent to the theorem stating that for natural numbers $n > 2$ the equation $x^4-4^{n-1} = y^n$ has no solution in rational numbers x, y, different from 0. To conclude this section we note that according to theorems of O. Korhonen [1], V. A. Lebesgue [1], W. Ljunggren [2], [3] and T. Nagell [2], [8], [9], [10] none of the equations $x^2+k = y^n$, where $0 < k \leqslant 10$, $k \neq 7$ has a solution in integers x, y for $n > 3$.

EXERCISES. **1.** Prove the theorem of V. Bouniakowsky [1] (of 1848) stating that for given coprime natural numbers m and n the equation

$$x^m t^n + y^m u^n = z^m v^n \tag{i}$$

has infinitely many solutions in natural numbers x, y, z, t, u, v.

PROOF. Let m, n be given natural numbers such that $(m, n) = 1$. In virtue of Theorem 16 of Chapter I there exist natural numbers r, s such that $mr-ns = 1$. Let a, b be arbitrary natural numbers and let $c = a+b$. It is easy to verify that the numbers

$$x = a^r, \quad y = b^r, \quad z = c^r, \quad t = b^s c^s, \quad u = a^s c^s, \quad v = a^s b^s$$

satisfy equation (i). □

2. Prove that the equation

$$x^2 = y^3+z^5$$

has infinitely many solutions in natural numbers.

PROOF. This is immediate: the numbers $x = n^{10}(n+1)^8$. $y = n^7(n+1)^5$, $z = n^4(n+1)^3$, where $n = 1, 2, \ldots$, satisfy the equation. □

3. Prove that for each natural number $n > 1$ the equation $x^n+y^n = z^{n-1}$ has infinitely many solutions in natural numbers x, y, z.

PROOF. This follows from the identity

$$((1+k^n)^{n-2})^n+(k(1+k^n)^{n-2})^n = ((1+k^n)^{n-1})^{n-1}$$

which holds whenever k, n are natural numbers, $n \geqslant 2$. □

4. Prove that for each natural number n the equation $x^n+y^n = z^{n+1}$ has infinitely many solutions in different natural numbers x, y, z.

PROOF. This follows from the identity

$$(1+k^n)^n+[k(1+k^n)]^n = (1+k^n)^{n+1}. \quad \square$$

REMARK. The equations $Ax^m+By^n = z^p$ and, more generally, $\sum_{i=1}^{n} A_i x_i^{g_i} = 0$ have been investigated by several authors, cf. Tchacaloff et Karanicoloff [1], Vijayaraghavan [1], Georgiev [1], Schinzel [12].

5. Prove, in connection with the Fermat Last Theorem, the following statement:

If n is a natural number greater than 2, then the equation $x^n+(x+1)^n = (x+2)^n$ has no solution in natural numbers x.

PROOF. Suppose that n is an odd number > 2; if for some natural x the equality $x^n+(x+1)^n = (x+2)^n$ holds, then, for $y = x+1$, we have $y^n = (y+1)^n-(y-1)^n$, whence

$$y^n-2\binom{n}{1}y^{n-1}-2\binom{n}{3}y^{n-3}-\ldots-2\binom{n}{n-2}y^2 = 2.$$

This proves that y^2 is a divisor of the number 2, which, by $y = x+1 > 1$, is impossible.

If n is an even number greater than 2, then, putting $y = x+1$, we obtain

$$y^n-2\binom{n}{1}y^{n-1}-2\binom{n}{3}y^{n-3}-\ldots-2\binom{n}{n-1}y = 0,$$

whence

$$y^{n-1}-2\binom{n}{1}y^{n-2}-2\binom{n}{3}y^{n-4}-\ldots-2n = 0.$$

The first equality shows that $y^n > 2ny^{n-1}$, whence $y > 2n$; the second equality shows that y is a divisor of $2n$; this is a contradiction. □

REMARK. B. Leszczyński [1] has proved that the only positive integers n, x, y, z, with $y > 1$ for which $n^x+(n+1)^y = (n+2)^z$ are: $n = 1$, x arbitrary, $y = 3, z = 2$ and $n = 3, x = y = z = 2$. The case $y = 1$ was settled by Dem'yanenko [4] and in a simpler way by Chein [1].

19. On some exponential equations and others

1. Equation $x^y = y^x$. We are going to find all the solutions of this equation in positive rational numbers x, y such that $x \neq y$. Suppose that x, y is such a solution and that $y > x$. Then $r = x/(y-x)$ is a positive rational number and $y = (1+1/r)x$. Therefore $x^y = x^{(1+1/r)x}$ and, since $x^y = y^x$, we have also $x^{(1+1/r)x} = y^x$, which proves that $x^{1+1/r} = y = (1+1/r)\,x$. Hence $x^{1/r} = 1+1/r$ and consequently

$$x = \left(1+\frac{1}{r}\right)^r, \quad y = \left(1+\frac{1}{r}\right)^{r+1}$$

Let $r = n/m$, where $(m, n) = 1$, and $x = t/s$, where $(t, s) = 1$. Since $x = \left(1+\frac{1}{r}\right)^r$, we have $\left(\frac{m+n}{n}\right)^{n/m} = \frac{t}{s}$, *whence* $\frac{(m+n)^n}{n^n} = \frac{t^m}{s^m}$. Each side of this equality is an irreducible fraction; for, in virtue of $(m, n) = 1$, we have $(m+n, n) = 1$, whence $((m+n)^n, n^n) = 1$, and, in virtue of $(t, s) = 1$, we have $(t^m, s^m) = 1$. It follows that $(m+n)^n = t^m$ and $n^n = s^m$. From this, in virtue of Corollary 1 to Theorem 16 of Chapter I, by $(m, n) = 1$, we infer that there exist natural numbers k and l such that $m+n = k^m, t = k^n$ and $n = l^m$, $s = l^n$. Therefore $m+l^m = k^m$. From this we deduce that $k \geqslant l+1$. If $m > 1$, we would have $k^m \geqslant (l+1)^m \geqslant l^m+ml^{m-1}+1 > l^m+m = k^m$, which is impossible. Consequently $m = 1$, whence $r = n/m = n$. This leads us to the conclusion that

$$x = \left(1+\frac{1}{n}\right)^n, \quad y = \left(1+\frac{1}{n}\right)^{n+1}, \tag{85}$$

where n is a natural number.

Conversely, it is easy to verify that the numbers x, y defined by (85) satisfy the equation $x^y = y^x$. Therefore *all the solutions of equation* $x^y = y^x$ *in rational numbers* x, y *with* $y > x > 0$ *are given by formulae* (85), *where* n *is a natural number.*

It follows that $n = 1$ is the only value for which the equation has a solution in natural numbers. In this case the solution is $x = 2$, $y = 4$.

Thus we arrive at the conclusion that *the equation* $x^y = y^x$ *has precisely one solution in natural numbers* x, y *with* $y > x$.

(This particular result can also be obtained in another way. It follows, e.g. from the fact that $\sqrt[3]{3} > \sqrt[2]{2} = \sqrt[4]{4} > \sqrt[5]{5} > \sqrt[6]{6} > \ldots > \sqrt[1]{1}$.)

The equation $x^y = y^x$, however, has infinitely many solutions in rational numbers x, y with $y > x$.

For $n = 2$ we find

$$\left(\frac{9}{4}\right)^{\frac{27}{8}} = \left(\frac{27}{8}\right)^{\frac{9}{4}}.$$

2. Equation $x^y - y^x = 1$. In virtue of the theorem of Moret-Blanc [1] *the equation*

$$x^y - y^x = 1 \tag{86}$$

has precisely two solutions in natural numbers. These are $x = 2, y = 1$ *and* $x = 3$, $y = 2$.

We present here a proof of this theorem.

Suppose that natural numbers x, y satisfy equation (86). Then, necessarily, $x^y > 1$, and therefore $x > 1$. If $x = 2$, then, by (86), $2^y = y^2+1$, which proves that y is odd and consequently $4 | y^2-1$. This implies that $4 | 2^y-2$ and $2 | 2^{y-1}-1$. We infer hence that $y = 1$.

We have

$$(87)\qquad \sqrt[3]{3} > \sqrt[2]{2} = \sqrt[4]{4} > \sqrt[5]{5} > \sqrt[6]{6} > \ldots > \sqrt[1]{1}.$$

In virtue of (86), $x^y > y^x$, $x^{1/x} > y^{1/y}$. The numbers $x = 3$, $y = 1$ do not satisfy equation (86) but the numbers $x = 3$, $y = 2$ do. Therefore, if x, y is a solution of equation (86) different from (2, 1) and (3, 2), then either $x = 3$, $y \geqslant 4$ or, by $x^{1/x} > y^{1/y}$ and (87), $x \geqslant 4$, $y \geqslant x+1$. Thus in either case we have $y \geqslant x+1$. Let $y-x = a$. Obviously a is a natural number and the equalities

$$(88)\qquad \frac{x^y}{y^x} = \frac{x^{x+a}}{(x+a)^x} = \frac{x^a}{\left(1+\dfrac{a}{x}\right)^x}$$

hold. But, as we know, $e^t > 1+t$ whenever $t > 0$, which implies that for $t = a/x$ we have $(1+a/x)^x < e^a$. Therefore, in virtue of (88) and by $x \geqslant 3 > e$, we obtain

$$\frac{x^y}{y^x} > \frac{x^a}{e^a} = \left(\frac{x}{e}\right)^a \geqslant \frac{x}{e} \geqslant \frac{3}{e} > 1.1.$$

Hence $x^y - y^x > \dfrac{y^x}{10} \geqslant \dfrac{4^3}{10} > 1$, contrary to the assumption that the pair (x, y) is a solution of equation (86). This leads us to the conclusion that equation (86) has no solution different from $x = 2$, $y = 1$ and $x = 3$, $y = 2$.

3. Equation $x^x y^y = z^z$. This equation has infinitely many solutions in natural numbers different from 1. As has been found by Chao Ko [2], for a natural number n the numbers

$$x = 2^{2^{n+1}(2^n-n-1)+2n}(2^n-1)^{2(2^n-1)},$$
$$y = 2^{2^{n+1}(2^n-n-1)}(2^n-1)^{2(2^n-1)+2},$$
$$z = 2^{2^{n+1}(2^n-n-1)+n+1}(2^n-1)^{2(2^n-1)+1}.$$

satisfy the equation $x^x y^y = z^z$. Thus, in particular, for $n = 2$ we obtain $x = 2^{12}\cdot 3^6 = 2985984$, $y = 2^8\cdot 3^8 = 1679616$, $z = 2^{11}\cdot 3^7 = 4478976$. Chao Ko has also proved that the equation $x^x y^y = z^z$ has no solution in natural numbers x, y, z each greater than 1 and such that $(x, y) = 1$.

V. A. Dem'yanenko [3] has proved that if x, y, z are natural numbers greater than 1 and satisfying the equation $x^x y^y = z^z$, then x, y must have the same sets of prime divisors (see, Chapter III, § 1).

We do not know whether the equation $x^x y^y = z^z$ has a solution in odd numbers greater than 1.

4. We conclude this paragraph with the equation

$$x!y! = z!.$$

It is not difficult to prove that the equation has infinitely many solutions in natural numbers x, y, z each greater than 1. To do this we observe that, if n is a natural number greater than 2, then the numbers $x = n!-1$, $y = n$, $z = n!$ satisfy the equation. Thus, in particular, for $n = 3$, we obtain $5!3! = 6!$. There is another solution of the equation which is not given by the formulae presented above.

Namely, we have $6!7! = 10!$. We do not know whether there exists any other such solution (see Guy [1], p. 44).

On the other hand, it is easy to find all the solutions of the equation $x!+y! = z!$ in natural numbers. In fact, if x, y, z is such a solution, then we may assume that $x \leqslant y$ and then $z > y$, i.e. $z \geqslant y+1$, whence $z! \geqslant (y+1)!$. But $z! = x!+y! \leqslant y!2$, whence $y!2 \geqslant (y+1)! = y!(y+1)$ and consequently $y+1 \leqslant 2$, i.e. $y = 1$, whence $x = 1$ and $z = 2$. We conclude that the equation $x!+y! = z!$ has precisely one solution in natural numbers x, y, z, namely $x = 1$, $y = 1$, $z = 2$. Some other equations involving factorials have been investigated by P. Erdös and R. Obláth [1] and also by R. M. Pollack and H. N. Shapiro [1].

CHAPTER III

PRIME NUMBERS

1. The primes. Factorization of a natural number m into primes

Any number > 1 which has no natural divisors except itself and 1 is called a *prime number*, or simply a *prime*. *A necessary and sufficient condition for a natural number* $m > 1$ *to be a prime is that* m *should not be the product of two natural numbers less than* m. In fact, if m is a prime, then it cannot be the product $a \cdot b$ of two natural numbers less than m, since, if it could, the numbers a and b would be greater than 1 and therefore the number m would have a divisor greater than 1 and less than m, which would contradict the assumption that m is a prime. This proves the necessity of the condition. On the other hand, if the number m is not a prime, then it has a divisor a such that $1 < a < m$ and hence $m = a \cdot b$, where b must be a natural number less than m, since $a > 1$. Thus the number m is the product of two natural numbers, each of them less than m. Thus the sufficiency of the condition is proved.

Thus the definition itself provides a method by means of which one can decide whether a given natural number $n > 1$ is a prime or not. In fact, it suffices to divide the number n by the numbers $2, 3, \ldots, n-1$ successively and see whether any of these numbers divides the number n; if none of them does, then (and only then) the number n is a prime.

A natural number which is neither 1 nor a prime is said to be *composite*. Such a number is representable as the product of two positive integers each less than the number in question. Consequently if n is a composite number, $n = ab$, where a and b are natural numbers each less than n; it follows that each of the numbers a, b is greater than 1. Interchanging, if necessary, the rôles of a and b, we may assume that $a \leqslant b$, whence $a^2 \leqslant ab = n$, and consequently $a \leqslant \sqrt{n}$. Hence we have

THEOREM 1. *If a natural number* n *is composite, then it has a divisor* a *such that* $1 < a \leqslant \sqrt{n}$.

It follows that in order to decide whether a natural number $n > 1$ is a prime it suffices to divide it by numbers greater than 1 and not greater than $\sqrt{n}$, successively.

We now prove

THEOREM 2. *Every natural number* > 1 *has at least one prime divisor.*

PROOF. Let n be a natural number > 1. Obviously the number n has some divisors greater than 1, since the number n itself is such a divisor. Denote by p the least of them. If p were not a prime, then we would have $p = ab$, where a, b would be natural numbers greater than 1 and less than p. Thus the number a would be a divisor of n at the same time greater than 1 and less than p, contrary to the definition of p. Therefore p is a prime and this completes the proof of Theorem 2. □

As an immediate consequence of Theorems 1 and 2 we have

COROLLARY 1. *Every composite number n has at least one prime divisor* $\leqslant \sqrt{n}$.

COROLLARY 2. *Every natural number* > 1 *is the product of a finite number of prime factors.* (Clearly, trivial products of one factor are not excluded).

PROOF. Suppose to the contrary that Corollary 2 is untrue. Then there exists a least natural number $n > 1$ which is not the product of prime numbers. In virtue of Theorem 2 number n has a prime divisor p and $n = pn_1$, where n_1 is a natural number. We cannot have $n_1 = 1$; for, in that case we would have $n = p$ and the Corollary 2 would be true.

Therefore $n_1 > 1$ and $n = pn_1 > n_1$. Hence $n_1 < n$, and from the definition of number n we infer that n_1 is the product of prime numbers. Then, however, the number $n = pn_1$ is also the product of prime numbers, contrary to the definition of number n. Thus the assumption that Corollary 2 is untrue results in a contradiction. Corollary 2 is thus proved. □

A question arises whether there exists a method which would enable us to represent a given natural number as a product of prime numbers. We show that, although the calculations involved may be very long, such a method does exist. It is sufficient to prove that for a given natural number one can either find the required factorization for the number n

itself or reduce the problem to finding such a factorization of a number less than n.

If n is a natural number > 1, then, dividing it by 2, 3, ..., n successively, we find its least divisor which, as we know, is a prime p. We then have $n = pn_1$, where n_1 is a natural number. If $n_1 = 1$, then $n = p$ and the desired representation is completed. If $n_1 > 1$, then in order to find the representation of n it suffices to find the representation for the number n_1, less than n. Continuing, we proceed similarly with n_1 in place of n. It is clear that after a finite number of steps less than n we ultimately obtain the representation of number n as a product

$$n = pp'p'' \dots p^{(k-1)}$$

of prime factors. If in this product some identical factors occur,then replacing them by the powers of suitable prime numbers we can rewrite the representation in the form

$$n = q_1^{a_1} q_2^{a_2} \dots q_s^{a_s}, \tag{1}$$

where $q_1, q_2, \dots, q_s$ are all different prime numbers, i.e. for instance, $q_1 < q_2 < \dots < q_s$ and a_i $(i = 1, 2, \dots, s)$ are natural numbers. Such representation of a natural number n is called the *factorization of n into prime numbers*.

In factorization (1) of number n the numbers $q_1, q_2, \dots, q_s$ are all the prime divisors of the number n. In fact, if the number n were divisible by a prime number q different from the numbers $q_1, q_2, \dots, q_s$, then, for $i = 1, 2, \dots, s$, we would have $(q, q_i) = 1$, since the prime number q has only two divisors, q and 1, and $q \neq q_i$. Therefore any two different prime numbers are relatively prime. We would also have $(q, q_i^{a_i}) = 1$ for $i = 1, 2, \dots, s$, whence, in virtue of (1) and Theorem 6ᵃ of Chapter I, $(q, n) = 1$, contrary to the assumption that n is divisible by q.

We see that the numbers q_i $(i = 1, 2, \dots, s)$, as well as the number of them, are uniquely determined by number n (as the prime divisors of n). Moreover, also the exponents $a_1, a_2, \dots, a_s$ are uniquely determined by n. In particular, the number a_1 can be defined as the greatest natural number for which $q_1^{a_1} \mid n$, since in the case $q_1^{a_1+1} \mid n$ we would have $q_1 \mid q_2^{a_2} \dots q_s^{a_s} \mid n$, which is impossible. Therefore, since we have assumed that $q_1, q_2, \dots, q_s$ is an increasing sequence, factorization (1) is unique.

This leads us to the following

THEOREM 3. *Any natural number can be represented in one and only one way as a product of primes. (Clearly enough two factorizations are regarded as being identical if they differ in the order of the factors).*

As has been proved above, for every natural number $n > 1$ we are able to find the factorization into primes effectively provided we are not daunted by long calculations, which may possibly occur.

In some cases these are too long to be carried out even with the aid of the newest technical equipment. For instance this happens in the case of the number $2^{293}-1$, which has 89 digits. (We know that this number is composite.) We do not know any of its prime divisors, although we do know that the least of them has at least 11 digits. We do not know any of the prime divisors of the number $F_{20} = 2^{2^{20}}+1$, either. It is not known whether this number is a prime or not. We know a prime divisor of the number F_{9448}, namely $19 \cdot 2^{9450}+1$, though we do not know any other of its prime divisors, which, as we know, do exist.

An example of a number which can easily be proved to be composite but none of whose prime divisors are known is the number F_{20}^2.

THEOREM 4. *If a natural number n is greater than* 2, *then between n and n! there is at least one prime number.*

PROOF. Since $n > 2$, the number $N = n!-1$ is greater than 1, whence, in virtue of Theorem 2, it has a prime divisor, p. Number p cannot be less than or equal to n. since, if it could, it would divide 1, which is impossible. Consequently $p > n$. On the other hand, $p \leqslant N$, p as a divisor of N. Thus we conclude that $n < p \leqslant n!-1 < n!$, which completes the proof. □

It follows that for each natural number n there exists a prime number greater than n; therefore there are infinitely many prime numbers. In particular, there exist prime numbers having at least hundred thousand digits, but we do not know any one of them. The greatest prime number which is known so far is the number $2^{216091}-1$; it has 65050 digits. The proof that it is a prime number was carried out in 1985.

EXERCISES. **1.** Given a prime each of whose digits (in the decimal expansion) equals 1, prove that the number of the digits must be prime. (The converse implication is not true).

PROOF. Let n be such a number having s digits in the decimal expansion, each equal to 1; suppose that s is a composite number, i.e. $s = ab$, where a, b are natural numbers, each greater than 1.

We then have $n = \frac{10^{ab}-1}{9} = \frac{10^{ab}-1}{9}$. But $10^a - 1 \mid 10^{ab}-1$, whence $\frac{10^a-1}{9} \,\Big|\, n$. $\frac{10^a-1}{9}$ is a natural number > 1, since $a > 1$. Since $b > 1$, we have $\frac{10^a-1}{9} < \frac{10^{ab}-1}{9} = n$.

From this we conclude that number n has a divisor $\frac{10^a-1}{9}$, less than n and greater than 1, which is impossible. This completes the proof.

To see that the converse implication does not hold we note, for example, that $111 = 3 \cdot 37$ and $11111 = 41 \cdot 271$. We do not know whether the sequence 11, 111, 1111,... contains infinitely many terms which are prime numbers. M. Kraïtchik [2] (Chapter III) has proved that number $(10^{23}-1)/9$ is a prime.

According to Williams and Dubner [1] for $p < 10000$ primes of the form $(10^p-1)/9$ are obtained only for p equal to 2, 19, 23, 317 and 1031. □

2. Prove that there exist infinitely many natural numbers which are not of the form a^2+p, where a is an integer and p a prime.

PROOF. Such are for instance the numbers $(3n+2)^2$, where $n = 1, 2, \ldots$ Suppose, to the contrary, that for a natural number n we have $(3n+2)^2 = a^2+p$, where a is an integer and p a prime. Then, plainly, a cannot equal 0; consequently, we may assume that a is a natural number. Then $3n+2 > a$, so $3n+2-a > 0$. But $p = (3n+2-a)(3n+2+a)$, whence $3n+2-a = 1$ and $3n+2+a = p$, which implies that $p = 6n+3 = 3(2n+1)$, which is impossible. □

REMARK. It can be proved that for every natural number k there are infinitely many k-th powers of natural numbers which are not of the form a^k+p, where a is an integer and p a prime. (cf. Clement [2]).

As verified by Euler, each odd natural number n, with $1 < n < 2500$, is of the form $n = 2a^2+p$, where a is an integer and p a prime. This is not true for n equal to 5777 and 5993, cf. Dickson [7], Vol. I, p. 424. I do not know whether there exist infinitely many odd natural numbers that are not of the form $2a^2+p$, where a is an integer and p a prime.

3. Prove that every number of the form 8^n+1 is composite.

PROOF. For each natural number n we have $2^n+1 \mid 2^{3n}+1 = 8^n+1$ and, clearly, $1 < 2^n+1 < 8^n+1$. This proves that the number 8^n+1 is composite. □

REMARK. We do not know whether there are infinitely many prime numbers of the form 10^n+1 ($n = 1, 2, \ldots$), or whether every number of the form 12^n+1 is composite ($n > 1$).

2. The Eratosthenes sieve. Tables of prime numbers

It is an immediate consequence of Corollary 1 of § 1 that, if a natural number $n > 1$ is not divisible by any prime number $\leqslant \sqrt{n}$, then n is a prime number.

It follows that in order to obtain all the prime numbers which occur in the sequence 2, 3, 4, ..., m, where m is a given natural number, it suffices to remove all the multiples kp of the prime numbers $p \leqslant \sqrt{m}$ with $k > 1$ from the sequence. Thus, in particular, to obtain all the primes occurring in the sequence 2, 3, ..., 100 it is sufficient to remove from the sequence all the numbers greater than 2, 3, 5 and 7 and divisible by at least one of these numbers.

An easy method of finding consecutive prime numbers was given by a Greek mathematician Eratosthenes. We consider the sequence 2, 3, 4, ... Then, since 2 is the first prime number p_1, we remove from the sequence all the numbers greater than p_1 and divisible by 2. The first of the remaining numbers is $3 = p_2$. We now remove all the numbers greater than p_2 and divisible by p_2. The first of the remaining numbers is $5 = p_3$. Suppose that after the nth step we have found the nth prime number p_n. We remove from the sequence all the numbers greater than p_n and divisible by p_n. The least number which has not yet been removed is the $(n+1)$-th prime number.

If the sequence of the natural numbers from 2 onwards is replaced by the sequence of natural numbers $2, 3, ..., N$, the above procedure terminates after the kth step, where p_k is the greatest prime number $\leqslant \sqrt{N}$.

Thus we obtain $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29$, $p_{25} = 97$, $p_{100} = 541$, $p_{200} = 1223$, $p_{1000} = 7917$, $p_{1229} = 9973$, $p_{1230} = 10007$. It has recently been computed that $p_{6000000} = 104395301$ (cf. Editorial Note [1]). D. Blanuša [1] has found the following simple geometric interpretation of the Eratosthenes sieve. In the Cartesian system of coordinates the set A of points $\left(0, \frac{1}{m}\right)$, $m = 1, 2, ...$, and the set B of points $(n+1, 0)$, $n = 1, 2, ...$, are considered. Each point of the set A is connected with each point of the set B by a straight line. Then the set of the abscissae of the intersections of the straight lines with the straight line $y = -1$ is precisely the set of composite numbers.

In fact, the equation of the line joining points $\left(0, \frac{1}{m}\right)$ and $(n+1, 0)$ is $x/(n+1) + my = 1$. This line intersects the line $y = -1$ at the point whose abscissa is $x = (m+1)(n+1)$. But, since m and n are natural numbers, x is a composite number. Conversely, if x is a composite number, then $x = (m+1)(n+1)$, where m, n are natural numbers, and consequently it is the abscissa of the intersection of the line joining the point $\left(0, \frac{1}{m}\right)$ and the point $(n+1, 0)$ with the line $y = -1$.

There exist printed tables of the prime numbers less than eleven milions, cf. D. N. Lehmer [1]. In that table for each natural number not greater than 10170000 the least prime divisor greater than 2, 3, 5, 7 is given. Cf. also Kulik, Poletti, Porter [1], where the primes of the eleventh milion are listed.

Jacob Philip Kulik, a mathematician of Polish origin (born in 1793 in Lwów, died in 1863 in Prague), prepared a manuscript (to the writing of which he devoted 20 years of his life) under the title *Magnus Canon Divisorum pro omnibus numeris par* 2, 3, 5 *non divisilibus et numerorum primorum interjacentium ad Millies centum millia, accuratius ad* 100330201 *usque. Authore Jacobo Philippo Kulik Galiciano Leopolensis Universitate Pragensi Matheseos sublimioris Prof. publ. ac ord.* At present the manuscript is owned by the Vienna Academy of Sciences. This manuscript was used when the table for prime numbers less than eleven millions were being prepared. (Some mistakes in it were then corrected.)

An article about J. P. Kulik and his work together with his portrait has recently been published by I. Ya. Depman [1]. For the history of tables of prime numbers, see ibid. pp. 594-601.

In 1959 C. L. Baker and F. J. Gruenberger made microcards containing all the prime numbers less than 104395301, cf. Baker and Gruenberger [1].

3. The differences between consecutive prime numbers

As in the preceding section let p_n denote the nth prime number and let $d_n = p_{n+1} - p_n$ for $n = 1, 2, \ldots$ The first hundred of the terms of the infinite sequence $d_1, d_2, \ldots$ are the following:

1, 2, 2, 4, 2, 4, 2, 4, 6, 2
6, 4, 2, 4, 6, 6, 2, 6, 4, 2
6, 4, 6, 8, 4, 2, 4, 2, 4, 14
4, 6, 2, 10, 2, 6, 6, 4, 6, 6
2, 10, 2, 4, 2, 12, 12, 4, 2, 4
6, 2, 10, 6, 6, 6, 2, 6, 4, 2
10, 14, 4, 2, 4, 14, 6, 10, 2, 4
6, 8, 6, 6, 4, 6, 8, 4, 8, 10
2, 10, 2, 6, 4, 6, 8, 4, 2, 4
12, 8, 4, 8, 4, 6, 12, 2, 18, 6

Number 2 is the only even number which is a prime (since even numbers greater than 2 are divisible by 2, they are composite). Thus numbers p_n for $n > 1$ are odd and, consequently, the numbers $d_n = p_{n+1} - p_n$ are even.

Looking at the table presented above (p. 119), one can raise the question whether for each natural number k there exists at least one number n for which $d_n = 2k$? We do not know the answer to this question.

We present here the table of the least natural numbers n for which $d_n = 2k$ with $2k \leqslant 30$ together with the prime numbers p_n, p_{n+1} such that $p_{n+1} - p_n = 2k$.

$2k$	n	p_n	p_{n+1}
2	2	3	5
4	4	7	11
6	9	23	29
8	24	89	97
10	34	139	149
12	46	199	211
14	30	113	127
16	282	1831	1847
18	99	523	541
20	154	887	907
22	189	1129	1151
24	263	1669	1693
26	367	2477	2503
28	429	2971	2999
30	590	4297	4327

(Cf. Lander and Parkin [3]).

It has been found that the least consecutive prime numbers whose difference is 100 are the numbers 396733 and 396833. The table of the numbers d_{n-1} with $n < 600$ has been given by P. Erdös, A. Rényi [1] (1). The table of d_n with $n \leqslant 1233$ has been given by M. Colombo [1].

The table of the least numbers p_n for which $p_{n+1} - p_n = 2k$ with $2k \leqslant 314$ has been given by Lander and Parkin [3] and Brent [1] (see also Brent [4], Weintraub [1])

Over a hundred years ago the conjecture was raised that for every even number $2k$ there exist infinitely many natural numbers n such that $d_n = 2k$ (de Polignac [1]). For $k = 2$ this conjecture is equivalent to the conjecture that there exist infinitely many pairs of *twin primes*, i.e. pairs of consecutive odd numbers n each of which is a prime. The first ten such pairs are 3 and 5, 5 and 7, 11 and 13, 17 and 19, 29 and 31, 41 and 43, 59 and 61, 71 and 73, 101 and 103, 107 and 109. H. Tietze has given a table of twin primes less than 300000 presenting the greater number of each pair. They are 2994 in number (Cf. Tietze [1] and also Früchtl [1]. See also Selmer and Nesheim [1], where the numbers n are given for which $6n+1$ and $6n-1$ are both prime and less than 200000. Compare also Sexton [1] and [2].) Brent [3] has found that there are 152892 pairs of twin primes less than 10^{11}. The greatest of the known pairs of twin primes is the pair $260497545 \cdot 2^{6625} \pm 1$ (Atkin and Rickert, see Yates [1]).

---

(1) There are some mistakes in the table (observed by J. Gałgowski and L. Kacperek):
instead of $d_{256} = 12$ it should be $d_{256} = 2$,
instead of $d_{314} = 6$ it should be $d_{314} = 4$,
instead of $d_{344} = 12$ it should be $d_{344} = 22$,
instead of $d_{429} = 18$ it should be $d_{429} = 28$,
instead of $d_{465} = 4$ it should be $d_{465} = 6$,
instead of $d_{462} = 18$ it should be $d_{462} = 28$.
It should be also $d_{579} = 2$.

It can be proved that the problem whether there exist infinitely many pairs of twin primes is equivalent to the question whether there exist infinitely many natural numbers n for which n^2-1 has exactly 4 natural divisors.

We note here that in order to obtain from the sequence of consecutive integers $1, 2, \ldots, n$ the prime numbers p for which also $p+2$ is prime one has to remove for each composite number k the number $k-2$ provided all the composite numbers have already been removed (for instance by means of the Erathostenes sieve) from this sequence (cf. Golomb [1]).

W. A. Golubew [2] has asked whether for a natural number n there is at least one pair of twin primes between n^3 and $(n+1)^3$.

It has been proved that the series of the reciprocals of the prime numbers of the pairs of twin primes is finite or convergent (Brun [1]) (¹).

The sum of the series

$$\left(\tfrac{1}{3}+\tfrac{1}{5}\right)+\left(\tfrac{1}{5}+\tfrac{1}{7}\right)+\left(\tfrac{1}{11}+\tfrac{1}{13}\right)+\left(\tfrac{1}{17}+\tfrac{1}{19}\right)+\left(\tfrac{1}{29}+\tfrac{1}{31}\right)+\ldots$$

has been calculated with an accuracy to six decimal places by Brent [2]. In § 14 we shall see that the series of the reciprocals of all the prime numbers is divergent.

Another question to which the answer is not known is whether there exist infinitely many primes p for which p, $p+2$, $p+6$ and $p+8$ are all prime numbers. A quadruple of the primes of this type is called simply a *quadruplet*. The first six consecutive quadruplets are obtained for $p = 5$, 11, 101, 191, 821, 1481. K. Früchtl [1], C. R. Sexton [3] and W. A. Golubew [1], [2], [3], [4] listed all quadruplets below 15000000, altogether 1209. It has been recently found by J. Bohman [2] that there are 49262 quadruplets below $2 \cdot 10^9$.

(¹) An "elementary" proof of the theorem of Brun is to be found in a book of E. Landau [2], vol. I.

It is easy to prove that for a given quadruplet such that the least of the primes it contains is greater than 5 any two numbers entering into it differ only in their least digits, which are 1, 3, 7 and 9, respectively. Clearly, each quadruplet forms two pairs of twin numbers.

However, there, are pairs of twin numbers not separated by a prime number which do not form a quadruplet. Such are the pairs 179, 181 and 191, 193, for instance. The latter forms a quadruplet with the pair 197, 199. The pairs of twin numbers 419, 421 and 431, 433 are not separated by any prime number; neither of them forms a quadruplet with any other pair of prime numbers. The pairs of twin numbers 809, 811; 821, 823 and 1019 1021; 1031, 1033 have the same property.

It seems a natural question to ask whether there exists an arbitrarily large number of consecutive pairs of twin numbers not separated by prime numbers. We know a number of triplets of such pairs. Such are for instance 179, 181; 191, 193; 197, 199 or 809, 811; 821, 823; 827, 829 or 3359, 3361; 3371, 3373; 3389, 3391 or 4217, 4219; 4229, 4231; 4241, 4243 or 6761, 6763; 6779, 6781; 6791, 6793. We also know an example of four such pairs: 9419, 9421; 9431, 9433; 9437, 9439; 9461, 9463.

It can be proved that if $p \neq 5$ and the numbers p, $p+2$, $p+6$ and $p+8$ are prime, then, dividing p by 210, we obtain 11, 101, or 191 as the remainder.

Turning back to the numbers d_n we note that it is easy to prove that they can be arbitrarily large. In fact, let m denote an arbitrary natural number greater than 1. Let p_n be the greatest prime number $\leqslant m!+1$. The numbers $m!+k$ are composite for $k = 2, 3, \ldots, m$ (since $k \mid m!+k$ for $k = 2, 3, \ldots, m$). Therefore $p_{n+1} \geqslant m!+m+1$ and consequently $d_n = p_{n+1} - p_n \geqslant m$.

On the other hand, we cannot prove that the numbers d_n $(n = 1, 2, \ldots)$ tend to infinity. There are natural numbers n such that $d_n = d_{n+1}$. For instance, $n = 2, 15, 36, 39, 46$. There are also natural numbers n for which $d_n = d_{n+1} = d_{n+2}$: for instance $n = 54, 464, 682, 709, 821, 829$. However we do not know whether for each natural number k there exists a natural number n such that $d_n = d_{n+1} = d_{n+2} = \ldots = d_{n+k}$ (see Lander and Parkin [4] and Bohman [2]).

P. Erdös and P. Turán [2] have proved that there exist infinitely many natural numbers n such that $d_n < d_{n+1}$ and also infinitely many numbers n for which $d_n > d_{n+1}$.

It has been proved that for every two natural numbers m and k there exists a natural number n such that each of the numbers $d_n, d_{n+1}, \ldots, d_{n+k}$

is greater than m. In other words, there exist arbitrarily many consecutive prime numbers such that the differences of the successive ones are arbitrarily large (Erdös [7]). The differences of consecutive prime numbers were the subject of extensive investigations by G. Ricci (cf. Ricci [1], [2]).

4. Goldbach's conjecture

Under this name the conjecture that every even number greater than 2 is the sum of two prime numbers is known. The conjecture has been verified directly for the even numbers up to 10^8 (Light, Forrest, Hammond, Roe [1]).

In 1973 Chen [2] proved that every sufficiently large even number is the sum of a prime and a natural number which has at most two prime factors. The first result of this kind was obtained by Brun [2] in 1920.

It follows from Goldbach's conjecture that every odd integer has infinitely many representations of the form $p+q-r$, where p, q, r are prime numbers. This result, not easy to prove, is due to J. G. van der Corput [2]. He also proved that almost every even number is a sum of two odd prime numbers. This means that for each positive number ε for every sufficiently large natural number N the number of even natural numbers $< N$ which fail to be sums of two primes is less than εN (van der Corput [1]).

According to A. Desboves [1] every natural number $\leqslant 10000$ of the form $4k+2$ is the sum of two primes, each being of the form $4k+1$. This of course could be true only if number 1 were regarded as a prime. Thus, in particular, $2 = 1+1$, $6 = 1+5$, $14 = 1+13$, $38 = 1+37$, $62 = 1+61$.

Another problem closely connected with the conjecture of Goldbach is whether for a given even natural number n the number $G(n)$ of all possible decompositions of n into the sum of two prime numbers increases to infinity together with the number n. N. Pipping [1], [2] has calculated the function $G(n)$ for even natural numbers n less than 5000 and some others. The calculation of $G(n)$ for $n \leqslant 2000000$ has been made by M. L. Stein and P. R. Stein (cf. Stein and Stein [1]). We have $G(4) = G(6) = 1$, $G(8) = 2$, $G(10) = 3$, $G(12) = 2$, $G(14) = 3$, $G(16) = G(18) = G(20) = 4$, $G(22) = 5$, $G(24) = 6$. Further, we have $G(158) = 9$ and the tables suggest that $G(2n) \geqslant 10$ for $2n > 158$. Similarly $G(188) = 10$ and it seems plausible that $G(2n) > 10$ for $2n > 188$. The least even number $2n$ for which $G(2n) \geqslant 100$ is 840; actually we have

$G(840) = 102$. The greatest number $2n$ for which $G(2n) < 100$ is probably the number $2n = 4574$.

It follows from the conjecture of Goldbach that each odd number greater than 7 is the sum of three odd primes. In fact, if n is an odd natural number > 7, then $n-3$ is an even number > 4. Consequently, in view of Goldbach's conjecture, it is the sum of two primes, each of them odd of course. Thus every odd natural number greater than 7 is the sum of three odd primes.

We do not know whether every odd number > 7 is the sum of three odd primes though the difficulty in solving this question is only of a technical nature, since I. Vinogradov proved in 1937 that for odd natural numbers greater than a certain effectively computable constant a the answer is positive. Later K. G. Borozdkin [1] proved that $a \leqslant \exp(\exp 16{,}038) < 3^{3^{15}}$. In view of this result it suffices to answer the problem for odd numbers n with $7 < n \leqslant a$, which for a given natural number is a matter of simple but perhaps tedious computations.

The situation is quite different as regards the question whether every even number is a difference of two prime numbers. Here no method of solution is known, even as tedious as that of the previous problem.

A. Schinzel [11] has proved that Goldbach's conjecture implies that every odd number > 17 is the sum of three different primes. It follows from the results of Vinogradov that each sufficiently large odd number is such a sum. The conjecture that every even number > 6 is the sum of two different prime numbers can also be proved to be equivalent to the conjecture that every natural number > 17 is the sum of three different prime numbers (Sierpiński [23]).

In 1930 L. Schnirelman [1] proved elementarily that there exists a number s such that every natural number > 1 is representable as the sum of at most s primes. Riesel and Vaughan [1] have proved by refining Schnirelman's method that every even natural number is the sum of at most 18 primes and hence every natural number > 1 is the sum of at most 19 primes. From the theorem of Vinogradov (quoted above) we see that every sufficiently large natural number is representable as the sum of at most four primes; the number of cases to be checked is however too great for a computer.

It can easily be proved that there exist infinitely many natural numbers which cannot be represented as the sums of less than three primes (compare Exercise 2 below).

It has also been conjectured that every odd number $n > 5$ is the sum of a prime number and a number of the form $2p$, where p is a prime (Dickson [7], vol. I, p. 424), Mayah [1] has verified it for $n < 42\cdot 10^5$.

EXERCISES. 1. Prove that every natural number > 11 is the sum of two composite numbers.

PROOF. Let n be a natural number greater than 11. If n is even, i.e. $n = 2k$, then $k \geqslant 6$ and $n-6 = 2(k-3)$, which, in view of the fact that $k \geqslant 6$, shows that $n-6$ is a composite number. If n is odd, i.e. $n = 2k+1$, then $k \geqslant 6$ and so $n-9 = 2(k-4)$ is a composite number. ☐

2. Prove that there exist infinitely many natural odd numbers which cannot be represented as the sum of less than three primes.

PROOF. Such are, for instance, the numbers $(14k+3)^2$, where $k = 1, 2, \ldots$ In fact, the numbers themselves are not primes. They cannot be represented as the sum of two primes either; for, if they could, then, since they are odd, one of the primes would be equal to 2, which would give $(14k+3)^2 = 2+p$, where p would be a prime. Hence $p = 7(28k^2+12k+1)$, which is impossible. ☐

REMARK. It can be proved elementarily that there exist infinitely many odd numbers which are sums of three different primes but are not sums of less than three different primes (cf. Sierpiński [31]).

3. Prove that the conjecture of Goldbach is equivalent to the conjecture that every even number > 4 is the sum of three prime numbers.

PROOF. It follows from Goldbach's conjecture that for a natural number $n > 1$ we have $2n = p+q$, where p and q are prime numbers. Hence $2(n+1) = 2+p+q$, that is, every arbitrarily chosen even number > 4 can be represented as the sum of three primes. On the other hand, if every even number > 4 is the sum of three primes, i.e., if for $n > 2$ we have $2n = p+q+r$, where p, q, r are primes, then at least one of the numbers p, q, r must be even, and consequently equal to 2. Suppose that, for instance, $r = 2$. Then $2(n-1) = p+q$ for $n-1 > 1$, which implies the conjecture of Goldbach. ☐

4. Prove that none of the equations $x^2+y^2 = z^2$, $x^2+y^2+z^2 = t^2$, $x^2+y^2+z^2+t^2 = u^2$ is solvable in prime numbers.

PROOF. For the first of the equations the result follows from the fact, proved in Chapter II, § 3, that for any solution of the equation in natural numbers at least one of the numbers must be divisible by 4.

Now suppose that there are primes x, y, z, t for which the equation $x^2+y^2+z^2 = t^2$ is satisfied. As was proved in Chapter II, § 10, at least two of the numbers x, y, z must be even; since they are primes, each of them is equal to 2. Thus $t^2-z^2 = 8$. But since z, t are primes and obviously odd ones, the equality $(t-z)(t+z) = 8$ implies that $t-z \geqslant 2$ and consequently $t+z \leqslant 4$, which is impossible, since t, z are odd primes.

Finally suppose that there exist primes x, y, z, t, u satisfying the equation $x^2+y^2+z^2+t^2 = u^2$. Clearly, the number u must be greater than 2, and thus it is odd. Therefore at least one of the numbers x, y, z, t must be odd. If precisely one of them were odd, say t, then we would have $x = y = z = 2$, whence $12+t^2 = u^2$ and consequently $(t-u)(t+u) = 12$, whence, since $t-u \geqslant 2$, $t+u \leqslant 6$. But this is impossible since u, t are different odd primes.

In the other case, i.e. if three of the primes x, y, z, t were odd, and the fourth of them were even, then $u^2 = x^2+y^2+z^2+t^2$ would be of the form $4k+3$, which is impossible. □

5. Find all the solutions of the equation $x^2+y^2+z^2+t^2+u^2 = v^2$ in primes x, y, z, t, u, v with $x \leqslant y \leqslant z \leqslant t \leqslant u \leqslant v$.

SOLUTION. There is precisely one such solution, namely $2^2+2^2+2^2+2^2+3^2 = 5^2$, for it is easy to prove that only one of the numbers x, y, z, t, u, can be odd. So we have $4 \cdot 2^2+u^2 = v^2$, whence $(v-u)(v+u) = 16$, $v-u \geqslant 2$, $v+u \leqslant 8$, so $u = 3$, $v = 5$.

5. Arithmetical progressions whose terms are prime numbers

Arithmetical progressions consisting of 18 different prime numbers are known, for instance $4808316343+71777060k$, for $k = 0, 1, 2, \ldots, 17$.

P.A. Pritchard [1] has found that the numbers $4180566390k + 8297644387$ ($k = 0, 1, 2, \ldots, 18$) form an arithmetical progression consisting of 19 different prime numbers. We do not know, however, whether there exists an arithmetical progression consisting of a hundred different prime numbers. We shall prove that if such a progression existed then the difference of its terms would have more than thirty digits.

To this end we prove the following theorem.

THEOREM 5. *If n and r are natural numbers, $n > 1$ and if n terms of the arithmetical progression $m, m+r, \ldots, m+(n-1)r$ are odd prime numbers, then the difference r is divisible by every prime number less than n* (cf. Dickson [7], vol. I, p. 425).

PROOF. Suppose that m, $n > 1$ and r are given natural numbers and that each of the numbers $m, m+r, \ldots, m+(n-1)r$ is an odd prime number. We must have $m \geqslant n$, since otherwise the composite number $m+mr = m(1+r)$ would be a term of the arithmetical progression. Let p denote a prime number less than n and let $r_0, r_1, \ldots, r_{p-1}$ be the remainders obtained by dividing the numbers $m, m+r, \ldots, m+(p-1)r$ by p, respectively. The latter are clearly less than p and moreover they are all different from zero, since otherwise one of the prime numbers being not less than $m \geqslant n > p$ would be divisible by the prime p, which is impossible.

Therefore the remainders can take only the values $1, 2, \ldots, p-1$, which are $p-1$ in number. From this we infer that for some two integers k and l such that $0 \leqslant k < l \leqslant p-1$ we have $r_k = r_l$. Consequently, $p \mid (m+lr) - (m+kr)$ and hence $p \mid (l-k)r$. But $0 < l-k \leqslant p-1 < p$, and therefore $p \mid r$. Since p was an arbitrary prime number less than n, the theorem follows. □

From Theorem 5 we derive the following

COROLLARY. *If there exists an increasing arithmetical progression consisting of $n > 2$ prime numbers, then the difference of this sequence is divisible by the product P_n of all the prime numbers less than n, and consequently it is $\geqslant P_n$.*

In particular, the difference of an arithmetical progression consisting of three different prime numbers must be $\geqslant P_3 = 2$. There exists precisely one arithmetical progression consisting of prime numbers whose difference is 2, namely 3, 5, 7.

It is known that there exist infinitely many arithmetical progressions consisting of three prime numbers each. The proof of this fact, however, is difficult (cf. van der Corput [2] and Chowla [2]).

The problem of the existence of infinitely many such arithmetical progressions is, clearly, equivalent to the question whether the equation $p+r = 2q$ has infinitely many solutions in prime numbers p, q, r, with $p \neq r$. It follows from the conjecture H (cf. § 8) that for every natural number n and every prime number $p \geqslant n$ there exist infinitely many increasing arithmetical progressions, each consisting of n terms which are prime numbers, the first term being p.

Here are now some examples of arithmetical progressions consisting of three prime numbers whose first terms are equal to 3: 3, 7, 11; 3, 11, 19; 3, 13, 23; 3, 17, 31; 3, 23, 43; 3, 31, 59; 3, 37, 71; 3, 41, 79; 3, 43, 83.

The difference of an arithmetical progression consisting of four prime numbers must be $\geqslant P_4 = 6$. There are known many arithmetical progressions consisting of four prime numbers each and having the difference equal to 6, e.g. 5, 11, 17, 23; 11, 17, 23, 29; 41, 47, 53, 59; 61, 67, 73, 79. It follows from the conjecture H that there are infinitely many such progressions, consisting, in addition, of consecutive prime numbers. In particular, such are the progressions 251, 257, 263, 269; 1741, 1747, 1753, 1759.

The difference of an arithmetical progression consisting of five different prime numbers must also be greater than or equal to 6. There exists precisely one arithmetical progression consisting of five different prime numbers whose difference is equal to 6. This is 5, 11, 17, 23, 29. To see that indeed there is precisely one such progression, we note that among five numbers forming an arithmetical progression whose difference is 6 one term must be divisible by 5. Similarly, we easily prove that there exists precisely one arithmetical progression consisting of five prime numbers whose difference is 12 — this is the progression 5, 17, 29, 41, 49 — and that there is no progression with the difference 18 or 24. However, it follows from the conjecture H that there exist infinitely many arithmetical progressions consisting of six prime numbers each and having the difference equal to 30. For example 7, 37, 67, 97, 127, 157; 541, 571, 601, 631, 661, 691.

It follows from the above corollary that in every arithmetical progression consisting of seven prime numbers the difference must be divisible by 30. It is easy to prove that there is no arithmetical progression consisting of seven primes whose difference is less than 150. However, there is precisely one arithmetical progression whose difference is 150; namely 7, 157, 307, 457, 607, 757, 907. The reason for this is that in every arithmetical progression consisting of seven natural numbers at least one of them must be divisible by 7.

In virtue of the corollary the difference of an arithmetical progression consisting of ten different prime numbers must be $\geqslant P_{10} = 210$. A progression whose difference is equal to 210 is formed by the numbers $199+210k$, where $k = 0, 1, 2, \ldots, 9$. It follows from the conjecture H that there are infinitely many such progressions.

In virtue of the corollary the difference of an arithmetical progression consisting of a hundred prime numbers would have to be divisible by the product of all prime numbers less than a hundred, and thus it would have more than thirty digits (in the scale of ten). We are not able to find, at least for the time being, any such arithmetical progressions. We do not know any proof of the existence of such an arithmetical progression either (cf. Grosswald and Hagis [1]).

6. Primes in a given arithmetical progression

Here is a problem on primes in arithmetical progressions of different type than those considered in § 5: for what natural numbers a and b does the arithmetical progression $ak+b$, $k = 1, 2, \ldots$, contain infinitely many prime numbers?

It is clear that, if $(a, b) = d > 1$, then there is no prime in the arithmetical progression $ak+b$, $k = 1, 2, \ldots$, because, for any k, $ak+b = d(ka/d+b/d)$ is a composite number (a/d, b/d are natural numbers). Therefore a necessary condition for the existence of infinitely many primes in an arithmetical progression $ak+b$ is that $(a, b) = 1$.

In the year 1837 Lejeune Dirichlet proved that this condition is also sufficient. The proof given by Lejeune Dirichlet is not elementary. Later the proof was simplified. The simplest proof of this theorem (though still very complicated) makes up Chapter VIII (p. 73–78) of the book by E. Trost [3].

We shall prove in the sequel several particular cases of this theorem: in Chapter V with $a = 4, b = 1, 3$ (Theorems 7 and 7a), in Chapter VI with $b = 1$, a being arbitrary (Theorem 11a), in Chapter IX with $a = 8$, $b = 3, 5, 7$ (Theorems 1, 2, 3) and with $a = 5$, $b = 4$ (Theorem 4).

The following two theorems are equivalent:

T. *If a and b are natural numbers such that $(a, b) = 1$, then there exist infinitely many primes of the form $ak+b$, where k is a natural number.*

T_1. *If a and b are natural numbers such that $(a, b) = 1$, then there exists at least one prime number p of the form $ak+b$ where k is a natural number* (¹).

PROOF. Trivially, T implies T_1. It is sufficient to prove the converse, that is, that T_1 implies T. We may suppose that $a > 1$ because for $a = 1$ the assertion follows from the fact that Theorem T holds. Let a, b be two given natural numbers such that $(a, b) = 1$. Then, of course, $(a^m, b) = 1$. Hence, by Theorem T_1, there exists a prime p such that $p = a^m k + b$, for a natural number k. But, since $a > 1, a^m \geqslant 2^m > m$. Hence $p > m$. Thus we have proved that for any natural number m there exists a prime of the form $ak+b$ which is greater than m. This shows that there exist infinitely many primes of this form. □.

It will be proved later (Chapter V, Theorem 9) that every prime of the form $4t+1$ is a sum of two perfect squares. Using this result we prove the following corollary of Theorem T:

COROLLARY. *For every natural number n there exists a prime p such that $p = a^2+b^2$, where a, b are natural numbers each greater than n.*

(¹) The proof of the equivalence of Theorems T and T_1 was given by me in the year 1950 (cf. Sierpiński [12], p. 526). Six years later the problem of the equivalence of Theorems T and T_1 was formulated in The Amer. Math. Monthly as E 1218 (1956), p. 342; and solved ibid. by D. Zeitlin (1957, p. 46), cf. V. S. Hanly [1].

PROOF. Let n be a natural number. According to T, there exists a prime $q > n$ which is of the form $4t-1$. Then, clearly

$$(4(1^2+q)^2(2^2+q)^2\dots(n^2+q)^2, q) = 1.$$

Hence, by Theorem T, we infer that there exists a natural number k such that the number

$$p = 4(1^2+q)^2(2^2+q)^2\dots(n^2+q)^2k-q$$

is a prime, necessarily of the form $4t+1$.

Thus the existence of the numbers a, b such that $p = a^2+b^2$, where $a < b$, is proved.

Suppose $a \leqslant n$. Then

$$\begin{aligned} b^2 = p-a^2 &= 4(1^2+q)^2(2^2+q)^2\dots(n^2+q)^2k-(a^2+q) \\ &= (a^2+q)\big(4(1^2+q)^2\dots((a-1)^2+q)^2((a+1)^2+q)\dots((n^2+q)^2k-1)\big), \end{aligned}$$

where both the factors on the right-hand side of the equality are relatively prime. Consequently they must be squares, but this is impossible because the second of the factors is of the form $4t-1$. Thus we come to the conclusion that $b > a > n$, and this completes the proof of the corollary. □

We note here that, according to a theorem of E. Hecke [1], for any two real numbers $c > d \geqslant 0$ there exists a prime p such that $p = a^2+b^2$ where a, b are natural numbers and $c > \frac{a}{b} > d$ (cf. Maknis [1]).

7. Trinomial of Euler x^2+x+41

It is easy to prove that there is no polynomial $f(x) = a_0x^m+a_1x^{m-1}+\dots+a_{m-1}x+a_m$ with integral coefficients and $a_0m > 0$ for which the numbers $f(x)$ would be prime for all integral values of x. In fact, as is well known, for sufficiently large x, say for $x > x_0$, the function $f(x)$ is increasing. If for some $x_1 > x_0$, $f(x_1) = p$ is a prime number, then as can easily be verified, $p \mid f(x_1+p)$, which, in virtue of $f(x_1+p) > f(x_1) = p$, implies that $f(x_1+p)$ is a composite number.

It has also been proved that there is no rational function whose all values would be prime numbers for all integral values of the argument except a constant function (Buck [1]).

However, there are polynomials of degree two with integral coefficients taking prime values for long sequence of consecutive natural numbers. For example such is the polynomial of Euler $f(x) = x^2+x+41$, whose values are prime numbers for $x = 0, 1, \ldots, 39$. To see this we note that $f(x+1) = f(x)+2(x+1)$. From this we easily infer that for $x = 0, 1, 2, \ldots$ the values $f(x)$ are the partial sums of the series $41+2\cdot 1+2\cdot 2+2\cdot 3+\ldots$ Thus we obtain the values 41, 43, 47, 53, 61, 71, 83, ..., 1601. As can be checked in the tables of prime numbers, each of these numbers is a prime. Since $f(-x) = f(x-1)$, also the numbers $f(-x)$ are prime for $x = 1, 2, \ldots, 40$. Thus for $x = -40, -39, \ldots, -1, 0, 1, \ldots, 39$ the function $f(x)$ takes the values which are all (not necessarily different) prime numbers. The function $f(x)$ has another interesting property: for integral values of x there is no divisor d with $1 < d < 41$ dividing $f(x)$.

In fact, suppose that for an integer x we have $d \mid f(x)$, where $1 < d < 41$. Let r be the remainder obtained by dividing x by d. Then $x = kd+r$, where k is an integer and $0 \leqslant r < d$. But since $f(kd+r) = kd(kd+2r+1)+f(r)$, the relation $d \mid f(x)$ implies $d \mid f(r)$; however this leads to a contradiction. In fact, in virtue of $0 \leqslant r < d < 41$, we must have $0 \leqslant r \leqslant 39$; therefore, as we know, $f(r)$ is a prime number $\geqslant 41$, and so it cannot have a divisor d such that $1 < d < 41$. Thus for an integer x the number $f(x)$ has no divisor d such that $1 < d < 41$.

This property is particularly relevant to finding whether for a given natural number $x \geqslant 40$ the number $f(x)$ is a prime. For $x = 40$ we have $f(40) = 40\cdot 41+41 = 41^2$, so the number $f(x)$ is composite. The number $f(41) = 41\cdot 42+41 = 41\cdot 43$ is also composite. If $x > 41$ and, if the number $f(x)$ is composite, then, by $(x+1)^2 = x^2+2x+1$ and $x^2+x+41 = f(x)$, we obtain $f(x) < (x+1)^2$. Therefore the number $f(x)$ has a prime divisor $p < x+1$ and, in virtue of what we proved above, $41 \leqslant p < x$ (since dividing $f(x)$ by x we obtain the remainder 41). Thus, in particular, the number $f(42) = 42\cdot 43+41$ is prime; for, plainly, it is not divisible by 41, the only prime number p for which $41 \leqslant p < 42$.

According to E. Trost ([3], p. 41), for x running up to 11000 the function $f(x)$ takes 4506 different values that are prime numbers.

We do not know whether in the sequence $f(x)$ $(x = 1, 2, \ldots)$ there are infinitely many prime numbers. (The answer in the affirmative follows from conjecture H, cf. § 8.)

It follows from the properties of the trinomial $f(x)$ that the trinomial $g(x) = f(x-40) = x^2-79x+1601$ takes values that are (not necessarily different) prime numbers for $x = 0, 1, 2, \ldots, 79$. (We have $g(t) = g(79-t)$ for all t.)

It follows from the work of G. Frobenius [1] and H. M. Stark [1] that there is no number A greater than 41 such that the trinomial x^2+x+A would take values which are prime numbers for $x = 0, 1, 2, \ldots, A-2$.

For $x = 0, 1, \ldots, 28$ the values taken by $6x^2+6x+31$ are all different prime numbers of the form $6k+1$; they are contained between 31 and 4909 with the limits included (C. Coxe, cf. van der Pol and Speziali [1]). The values of the binomial $2x^2+29$ are prime numbers for $-28 \leqslant x \leqslant 28$.

It can easily be proved that there exist polynomials of degree n taking prime values for $x = 0, 1, \ldots, n$; however we do not know any polynomial of degree two or higher in variable x about which we could prove that it takes prime values for infinitely many values of x. In particular, we do not know whether the binomial x^2+1 has this property. W. A. Golubew [5] has presented a list of all natural numbers $x \leqslant 120000$ for which the numbers x^2+1 are prime. M. Wunderlich [2] has found that there are 624535 numbers $x \leqslant 14\cdot 10^6$ with this property. H. Iwaniec [1] has proved that there exist infinitely many numbers x^2+1 composed of at most 2 primes and B. M. Bredihin [1] has proved that there exist infinitely many primes of the form x^2+y^2+1.

If a polynomial $f(x)$ with integral coefficients takes prime number values for infinitely many x's, then, plainly, the coefficient a_0 at the highest power of variable x must be positive, since for sufficiently large values of x the polynomial has the same sign as a_0. Furthermore, the polynomial $f(x)$ cannot be the product of two polynomials with integral coefficients, since otherwise for sufficiently large values of x the number $f(x)$ would be composite. Therefore the polynomial $f(x)$ is irreducible. However, these conditions are not yet sufficient for $f(x)$ to take values which are prime numbers even for at least one value of x. In fact, the polynomial x^2+x+4 is irreducible (it has no real root) and for all integers x the numbers x^2+x+4 are composite — they are even natural numbers greater than 3, since, as we know, the number $x^2+x = (x+1)x$ is even and non-negative.

In 1857 W. Bouniakowsky [2] formulated the following conjecture:

If $f(x)$ is an irreducible polynomial with integral coefficients and if N denotes the greatest common divisor of the numbers $f(x)$, x running over all integers, then the polynomial $f(x)/N$ takes prime number values for infinitely many x's (cf. Dickson [7], vol. I, p. 333).

For instance, consider the polynomial $f(x) = x^2+x+4$. Since $f(0) = 4$, $f(1) = 6$ and, as we already know, $f(x)$ is an even integer for integer x, then for x running over all integers the greatest common divisor of the numbers $f(x)$ is 2. Consequently it follows from the conjecture of Bouniakowsky, that for infinitely many integers x the number $x(x+1)/2+2$ is prime.

8. The Conjecture H

Let s denote a natural number and let $f_1(x), f_2(x), \ldots, f_s(x)$ be polynomials whose coefficients are integers. Suppose that there exist infinitely many natural numbers x for which each of the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ is a prime. As we learned in § 7, the polynomials $f_i(x)$, $i = 1, 2, \ldots, s$, must be irreducible and the leading coefficient of each of them must be positive. Accordingly, for sufficiently large values of x all the numbers $f_i(x)$, $i = 1, 2, \ldots, s$, can be arbitrarily large. As can easily be verified, this implies that there is no natural number $d > 1$ which divides the number $P(x) = f_1(x)f_2(x)\ldots f_s(x)$ for any natural value of x. In fact, if such a number could exist, it would be the divisor of the product of s arbitrarily large prime numbers, which is impossible.

We have thus proved that if s is a natural number and $f_1(x), f_2(x), \ldots, f_s(x)$ are polynomials whose coefficients are integers and if for infinitely many natural numbers x the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ are prime, then the polynomials must satisfy the following condition:

CONDITION C. *Each of the polynomials $f_i(x)$ $(i = 1, 2, \ldots, s)$ is irreducible, its leading coefficient is positive and there is no natural number $d > 1$ that is a divisor of each of the numbers $P(x) = f_1(x)f_2(x)\ldots f_s(x)$, x being an integer.*

In 1958 A. Schinzel formulated the following conjecture:

CONJECTURE H. *If s is a natural number and if $f_1(x), f_2(x), \ldots, f_s(x)$ are polynomials with integral coefficients satisfying Condition C, then there exist infinitely many natural values of x for which each of the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ is prime* (cf. Schinzel et Sierpiński [3], p. 188).

For the case of linear polynomials f_i an equivalent conjecture was formulated earlier by L. E. Dickson [1].

We present here some of the corollaries which follow from Conjecture H.

Let n be a given natural number and let $f_1(x) = x^{2^n}+1, f_2(x) = x^{2^n}+3$, $f_3(x) = x^{2^n}+7, f_4(x) = x^{2^n}+9$. For $P(x) = f_1(x)f_2(x)f_3(x)f_4(x)$ we have $P(0) = 1\cdot 3\cdot 7\cdot 9$ and $P(1) = 2\cdot 4\cdot 8\cdot 10$.. Consequently, $(P(0), P(1)) = 1$. Therefore Condition C is satisfied and Conjecture H gives the following corollary:

For every natural number n there exist infinitely many natural numbers x for which each of the numbers $x^{2^n}+1$, $x^{2^n}+3$, $x^{2^n}+7$, $x^{2^n}+9$ *is a prime* (Sierpiński [34]).

This implies that there exist infinitely many quadruplets of prime numbers (cf. § 3), and that there are infinitely many prime numbers of the form x^2+1 as well as of the form x^4+1. W. A. Golubew [6] has calculated that there are only five natural numbers x less than ten thousand for which each of the numbers x^2+1, x^2+3, x^2+7, x^2+9 is a prime. These are $x = 2, 10, 1420, 2080, 2600$.

Now let k denote an arbitrary integer and let $f_1(x) = x, f_2(x) = x+2k$. For $P(x) = f_1(x)f_2(x)$ we have $P(1) = 2k+1$, $P(2) = 4(k+1)$. Since clearly $(2k+1, 4(k+1)) = 1$, the polynomials satisfy Condition C. Consequently, according to Conjecture H, there exist infinitely many natural numbers x for which the numbers $p = x$ and $q = x+2k$ are both prime numbers. Hence $2k = p-q$, which proves that the number $2k$ admits infinitely many representations as the difference of two prime numbers. This means that the Conjecture H implies that every even number has infinitely many representations as the difference of two prime numbers. It can also be deduced from Conjecture H that every even number has infinitely many representations as the difference of two consecutive prime numbers (cf. Schinzel and Sierpiński [3], p. 190).

It follows from Conjecture H that if a and b are natural numbers such that $(a, b) = (a, b(b+2)) = 1$, then there exist infinitely many prime numbers p of the form $ak+b$, where k is a natural number, such that $p+2$ is a prime number. In fact, let $f_1(x) = ax+b$, $f_2(x) = ax+b+2$. For $P(x) = f_1(x)f_2(x)$ we have $P(0) = b(b+2)$, $P(1) = (a+b)(a+b+2)$ and $P(1)+P(-1) = 2a^2+2b(b+2)$. If there exists a prime number q such that $q \mid P(x)$ for all integers x, then, if b is odd, $P(0)$, and consequently q, are odd; and if b is even, then, in view of $(a, b) = 1$, a is odd; thus both $a+b$ and $a+b+2$ are odd and, consequently, $P(1)$ is odd, which implies that also q is odd. Therefore, in any case, q is odd. Since we have assumed that $q \mid P(0)$, i.e. $q \mid b(b+2)$ and $q \mid P(1)+P(-1)$, we have $q \mid 2a^2$ and consequently, since q is odd, $q \mid a$. But this is impossible since $(a, b(b+2)) = 1$. Thus we see that Condition C is satisfied. Therefore it follows from Conjecture H that there exist infinitely many natural numbers x for which the numbers $f_1(x) = ax+b$ and $f_2(x) = ax+b+2$ are prime. The corollary is thus proved.

It is easy to see that the condition $(a, b(b+2)) = 1$ is also necessary for the existence of infinitely many prime numbers p of the form $ak+b$ for which also the number $p+2$ is a prime.

Let k be an arbitrary integer and let $f_1(x) = x$, $f_2(x) = 2k+1+2x$. For $P(x) = f_1(x)f_2(x)$ we have $P(1) = 2k+3$, $P(-1) = -(2k-1)$. Since $(2k-1, 2k+3) = 1$ for every integer k, we see that the polynomials satisfy Condition C. Then, according to Conjecture H, there exist infinitely many natural numbers x for which the numbers $q = x$ and $p = 2k+1+2x$ are both prime.

Hence $2k+1 = p-2q$. Thus Conjecture H implies that every odd integer (>0 or <0) has infinitely many representations as the difference of a prime number and the double of a prime number.

G. de Rocquigny [1] has asked whether every integer divisible by 6 is the difference of two primes of the form $6k+1$. The positive answer to this is a corollary of Conjecture H. In fact, for $f_1(x) = 6x+1$ and $f_2(x) = 6x+6k+1$, $P(x) = f_1(x)f_2(x)$ we have $P(0) = 6k+1$, $P(-k) = -(6k-1)$ and, as is known, $(6k-1, 6k+1) = 1$ for all integers k.

It follows from Conjecture H that there exist arbitrarily long arithmetical progressions whose terms are consecutive prime numbers (cf. Schinzel and Sierpiński [3], p. 191).

There are many other corollaries which can be derived from Conjecture H, e.g. the conjecture of Bouniakowsky (cf. Schinzel and Sierpiński [3] and Schinzel [13]).

EXERCISE. Prove that Conjecture H implies the following assertion. Given two relatively prime integers a and b such that one of them is even and $a > 0$. Then there exist infinitely many prime numbers p such that $ap+b$ is a prime.

PROOF. Let $f_1(x) = ax+b$, $f_2(x) = x$. For $P(x) = f_1(x)f_2(x)$ we have $P(1) = a+b$, $P(-1) = a-b$, and since one of the numbers a, b is even, the other, in virtue of $(a, b) = 1$, is odd and so from $(a, b) = 1$ it follows that $(a+b, a-b) = 1$. Therefore $(P(1), P(-1)) = 1$ and this shows that Condition C is satisfied. Consequently, from Conjecture H we conclude that there exist infinitely many x for which both $f_2(x) = x$ and $f_1(x) = ax+b$ are prime numbers, and this is what was to be proved.

9. The function $\pi(x)$

For any real number x we denote by $\pi(x)$ the number of primes not greater than x. We then have $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = \pi(6) = 3$, $\pi(7) = \pi(8) = \pi(9) = \pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10000) = 1229$, $\pi(10^5) = 9592$, $\pi(10^6) = 78498$, $\pi(10^7) = 664579$, $\pi(10^8) = 5761455$, $\pi(10^9) = 50847534$.

In 1972 J. Bohman [1] calculated that $\pi(10^{10}) = 455052511$ (this was a correction of the result of Lehmer [8] obtained in 1958), $\pi(10^{11}) = 4118054813$, $\pi(10^{12}) = 37607912018$. Recently J. C. Lagarias, V. S. Miller and A. M. Odlyzko [1] have computed that $\pi(10^{13}) = 346065536839$ (this is a correction of a result of Bohman [1]), $\pi(10^{14}) = 3204941750802$, $\pi(10^{15}) = 29844570422669$ and $\pi(10^{16}) = 279238341033925$.

Obviously we have $\pi(p_n) = n$ for $n = 1, 2, \ldots$ P. Erdös has found (cf. Trost [3], pp. 52-53) quite an elementary proof of the inequality

$$\pi(n) \geqslant \frac{\log n}{2\log 2} \quad \text{for} \quad n = 1, 2, \ldots \tag{2}$$

As we proved in Chapter I, § 14, every natural number has a unique representation in the form k^2l, where k and l are natural numbers and, moreover, the number l is square-free. For each of the n numbers $1, 2, \ldots, n$, we have $k^2l \leqslant n$; so *a fortiori*, $k^2 \leqslant n$. Therefore $k \leqslant \sqrt{n}$. Consequently the number k can take at most $\sqrt{n}$ different values. The numbers l, being square-free and less than n, can be represented as products of different primes each not greater than n, i.e. as products of primes belonging to the sequence $p_1, p_2, \ldots, p_{\pi(n)}$. The number of such products (including number 1) is $2^{\pi(n)}$. Consequently the numbers l can assume at most $2^{\pi(n)}$ different values. Therefore the number of the products lk^2 (where l is square-free) each being not greater than n, is at most $\sqrt{n}\,2^{\pi(n)}$. Since every natural number $\leqslant n$ is representable as such a product, we have $n \leqslant \sqrt{n}\,2^{\pi(n)}$. Hence $\sqrt{n} \leqslant 2^{\pi(n)}$ and, further, taking the logarithm of both sides of the last inequality, we obtain $\frac{1}{2}\log n \leqslant \pi(n)\log 2$, which proves formula (2).

Later on (in § 14) we shall prove stronger inequalities for the function $\pi(n)$. The main interest in inequality (2), however, is aroused by the simplicity of its proof.

Let k denote an arbitrary natural number and let $n = p_k$. By formula (2), in view of $\pi(p_k) = k$, we have $k \geqslant \log p_k/2\log 2$. Therefore $p_k \leqslant 2^{2k}$

for $k = 1, 2, \ldots$, which, in virtue of the fact that 2^{2k} is a composite number for every $k = 1, 2, \ldots$, proves the inequality

$$p_k < 2^{2k} \quad \text{for} \quad k = 1, 2, \ldots \tag{3}$$

EXERCISES. 1. Prove that for natural numbers $n > 1$ the inequality

$$\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n} \tag{4}$$

holds if and only if n is a prime. For n being composite numbers we have

$$\frac{\pi(n-1)}{n-1} > \frac{\pi(n)}{n}. \tag{5}$$

PROOF. If n is a composite number, then $\pi(n) = \pi(n-1)$ and inequality (5) follows. If n is a prime number, then $\pi(n) = \pi(n-1)+1$, whence

$$\frac{\pi(n)}{n} - \frac{\pi(n-1)}{n-1} = \frac{1}{n}\left(1 - \frac{\pi(n-1)}{n-1}\right). \tag{6}$$

But since $\pi(k) < k$ for $k = 1, 2, \ldots$, (6) implies (4). ☐

2. Given a natural number m, find all the solutions of the equation $\pi(n) = m$ in natural numbers n.

SOLUTION. These are the natural numbers n for which $p_m \leqslant n < p_{m+1}$. Thus for a given natural number m there are $p_{m+1} - p_m$ solutions.

10. Proof of Bertrand's Postulate (Theorem of Tchebycheff)

For a given real number x we denote by $[x]$ the greatest integer $\leqslant x$. Thus, in particular, we have $[\frac{3}{4}] = 0$, $[-\frac{3}{4}] = -1$, $[\sqrt{2}] = 1$, $[\pi] = 3$. It follows from the definition that for all real numbers x we have $x-1 < [x] \leqslant x$. The equality $[x] = x$ holds if and only if x is an integer. If k is an integer, then for the x's that are real numbers we have $[x+k] = [x] + k$. For any real numbers x, y we have, of course, $[x]+[y] \leqslant [x+y]$. E.g.

$$0 = [\tfrac{1}{2}] + [\tfrac{2}{3}] < [\tfrac{1}{2} + \tfrac{2}{3}] = 1 \quad \text{but} \quad [\tfrac{1}{3}] + [\tfrac{1}{2}] = [\tfrac{1}{3} + \tfrac{1}{2}] = 0.$$

THEOREM 6. *The exponent of a prime p in the factorization into prime numbers of $n!$, where n is a natural number, is*

$$a = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots \tag{7}$$

PROOF. Let n, k be two given natural numbers and p a prime number $\leqslant n$. The numbers of the sequence $1, 2, \ldots, n$ which are divisible by p^k are of the form lp^k, where l is a natural number such that $lp^k \leqslant n$, that is $l \leqslant n/p^k$. The number of l's is, of course, $[n/p^k]$. On the other hand, it is clear that exponent a of the prime p in factorization into prime numbers of the number $n!$ is obtained by adding to the number of the terms of the sequence $1, 2, \ldots, n$ which are divisible by p the number of the terms divisible by p^2 and then the number of the terms divisible by p^3 and so on. This gives formula (7). □

As a simple application of Theorem 6 we calculate the number of zeros at the end of the number 100!.

According to formula (7) (for $n = 100$ and $p = 2$) the exponent of the number 2 in the factorization into prime numbers of the number 100! is

$$\left[\frac{100}{2}\right] + \left[\frac{100}{2^2}\right] + \left[\frac{100}{2^3}\right] + \ldots = 50+25+12+6+3+1 = 97.$$

The exponent of number 5 is

$$\left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] = 20+4 = 24.$$

Hence it follows that number 100! has 24 zeros at the end in its decimal expansion.

LEMMA 1. *For natural numbers $n > 1$ we have*

$$\binom{2n}{n} > \frac{4^n}{2\sqrt{n}}. \tag{8}$$

PROOF. Inequality (8) holds for $n = 2$ because $\binom{4}{2} = 6 > \dfrac{4^2}{2\sqrt{2}}$. Suppose that inequality (8) holds for a natural number $n > 1$. We then have

$$\binom{2n+2}{n+1} = 2\frac{2n+1}{n+1}\binom{2n}{n} > \frac{2(2n+1)4^n}{(n+1)2\sqrt{n}}$$
$$= \frac{2(2n+1)4^n}{\sqrt{4n(n+1)}\sqrt{n+1}} > \frac{4^{n+1}}{2\sqrt{n+1}},$$

for, since $(2n+1)^2 > 4n(n+1)$, we infer that $2n+1 > \sqrt{4n(n+1)}$. From this the proof of inequality (8) for $n > 1$ follows by induction. □

LEMMA 2. *The product P_n of the prime numbers $\leqslant n$, where n is a natural number, is not greater than 4^n.*

PROOF. The lemma is of course true for $n = 1$ and $n = 2$. Let n denote a natural number > 2. We suppose that the lemma holds for the natural numbers $< n$. If n is an even number > 2, then $P_n = P_{n-1}$. Hence the lemma holds for the number n. If, however, $n = 2k+1$, where k is a natural number, then each prime number p such that $k+2 \leqslant p \leqslant 2k+1$ is a divisor of the number

$$\binom{2k+1}{k} = \frac{(2k+1)\,2k\,(2k-1)\ldots(k+2)}{1\cdot 2\ldots k}. \tag{9}$$

In view of the fact that

$$(1+1)^{2k+1} > \binom{2k+1}{k} + \binom{2k+1}{k+1} = 2\binom{2k+1}{k},$$

we have

$$\binom{2k+1}{k} < 4^k.$$

Consequently, the product of all the (different) prime numbers such that $k+2 \leqslant p \leqslant 2k+1$ is a divisor of number (9) not greater than 4^k. But since, by the assumption that the lemma is valid for numbers less then n, the product of the prime numbers $\leqslant k+1$ is less than 4^{k+1}, we have $P_n = P_{2k+1} < 4^k \cdot 4^{k+1} = 4^{2k+1} = 4^n$. Hence $P_n < 4^n$. Thus, by induction, the lemma follows. □

LEMMA 3. *If p is a prime divisor of the number $\binom{2n}{n}$ with $p \geqslant \sqrt{2n}$, then the exponent of p in the factorization into primes of the number $\binom{2n}{n}$ is equal to* 1.

PROOF. By Theorem 6 the exponent of the prime p in the factorization into primes of the number $(2n)!$ is $\left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \left[\frac{2n}{p^3}\right] + \ldots$ and in the factorization of the number $n!$ the exponent of a prime p is $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$

In virtue of

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

the exponent of the prime p in the factorization into prime numbers of the number $\binom{2n}{n}$ is

$$a = \sum_{k=1}^{\infty}\left[\frac{2n}{p^k}\right] - 2\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right).$$

If $p \geqslant \sqrt{2n}$, then $p = \sqrt{2n}$ only in the case where $n = 2$. Therefore for $n \neq 2$ we have $p > \sqrt{2n}$, whence $a = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] < 2$. Consequently, $a < 2$, that is $a \leqslant 1$ (since a is an integer). This proves Lemma 3 for $n \neq 2$. For $n = 2$, however, we verify it directly; we have $\binom{4}{2} = 2 \cdot 3$.

LEMMA 4. *Each divisor of the number $\binom{2n}{n}$ which is of the form p^r, p being a prime and r a natural number, is not greater than $2n$. We have*

$$\binom{2n}{n} \leqslant (2n)^{\pi(2n)}.$$

PROOF. For a prime p such that $p^r \mid \binom{2n}{n}$, the exponent of p in the factorization of $\binom{2n}{n}$ into primes is

$$a = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \geqslant r.$$

If p^r were $> 2n$, then we would have $\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] = 0$ for $k \geqslant r$; consequently

$$a = \sum_{k=1}^{r-1}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right).$$

But since, for all real x, $[2x] - 2[x] \leqslant 1$, the last equality would imply that $a \leqslant r-1$, which contradicts the fact that $a \geqslant r$. Therefore $p^r \leqslant 2n$. To prove the second part of the lemma we note that since in the factorization of the number $\binom{2n}{n}$ only primes $\leqslant 2n$ can occur, we have $\binom{2n}{n} \leqslant (2n)^{\pi(2n)}$. The lemma is thus proved. □

LEMMA 5. *If n is a natural number > 2, then none of the primes p for which $\frac{2}{3}n < p \leqslant n$ can be a divisor of the number* $\binom{2n}{n}$.

PROOF. If $\frac{2}{3}n < p \leqslant n$, then $\frac{2n}{p} < 3$ and $\frac{n}{p} \geqslant 1$. Therefore $\left[\frac{2n}{p}\right] \leqslant 2$, $\left[\frac{n}{p}\right] \geqslant 1$, which gives $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 0$ (^{1}). For $k > 1$ we then have $p^k > \frac{4}{9}n^2$ and consequently $\frac{2n}{p^k} < \frac{9}{2n} < 1$ for $n > 4$. Therefore $\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] = 0$ for all $k > 1$ and $n > 4$. Hence we conclude that for $n > 4$ the exponent of the prime p in the factorization into primes of number $\binom{2n}{n}$ is zero, which means that $\binom{2n}{n}$ is not divisible by p. This proves the lemma for $n > 4$. To prove it for the remaining cases, that is for $n = 3$ and $n = 4$ we check that the inequalities $\frac{2}{3}n < p \leqslant n$ imply $p = 3$ and that 3 is not a divisor either of $\binom{6}{3} = 20$ or of $\binom{8}{4} = 70$. Lemma 5 is thus proved. □

LEMMA 6. *The exponent of a prime number p such that $n < p < 2n$ in the factorization into primes of the number $\binom{2n}{n}$ is equal to* 1.

PROOF. For $n < p < 2n$ we have $1 < \frac{2n}{p} < 2$, $\frac{n}{p} < 1$. Therefore $\left[\frac{2n}{p}\right] = 1$, $\left[\frac{n}{p}\right] = 0$, For $k \geqslant 2$ we have $\frac{2n}{p^k} \leqslant \frac{2n}{p^2} < \frac{2}{n}$. Therefore, for $n > 1$,

---

(^{1}) In fact for real numbers x we have $2[x] \leqslant 2x$, $[2x] > 2x-1$, whence $[2x] - 2[x] > -1$, and consequently, since the left-hand side is an integer, we have $[2x] - 2[x] \geqslant 0$.

$\dfrac{2n}{p^k} < 1$ and, consequently, $\left[\dfrac{2n}{p^k}\right] = 0$, whence of course $\left[\dfrac{n}{p^k}\right] = 0$. Hence the exponent a of the prime p in the factorization of the number $\binom{2n}{n}$ into primes is equal to 1. Clearly, for $n = 1$ there is nothing to prove, since $n < p < 2n$ cannot hold for $n = 1$. The lemma is thus proved. ☐

LEMMA 7. *For natural numbers* $n \geqslant 14$ *we have* $\pi(n) \leqslant \frac{1}{2}n-1$.

PROOF. As can easily be verified, we have $\pi(14) = 6 = \frac{14}{2}-1$. Consequently Lemma 7 is true for $n = 14$. Suppose that n is a natural number not less than 15. In the sequence $1, 2, \ldots, n$ the even numbers $4, 6, 8, \ldots, 2\left[\dfrac{n}{2}\right]$ are composite. Their number is clearly $\left[\dfrac{n}{2}\right]-1$. Moreover, in the sequence $1, 2, \ldots, n$ for $n \geqslant 15$, there are numbers which are odd, but not prime, namely 1, 9, 15. Thus

$$\pi(n) \leqslant n-\left(\left[\frac{n}{2}\right]-1+3\right) = n-\left[\frac{n}{2}\right]-2 < \frac{n}{2}-1$$

(because $\left[\dfrac{n}{2}\right] > \dfrac{n}{2}-1$). Thus $\pi(n) < \dfrac{n}{2}-1$ for $n \geqslant 15$, and this completes the proof of the lemma. ☐

LEMMA 8. *Let* R_n *denote the product of the primes* p *such that* $n < p \leqslant 2n$. *In the case when there are no such primes, let* $R_n = 1$. *Then*

$$R_n > \frac{4^{n/3}}{2\sqrt{n}\,(2n)^{\sqrt{n/2}}} \tag{10}$$

holds for all $n \geqslant 98$.

PROOF. If follows immediately from the definition of R_n that $R_n \mid \binom{2n}{n}$. Consequently $\binom{2n}{n} = Q_n R_n$, where Q_n is a natural number. Hence, by Lemma 6, we infer that none of the numbers p with $n < p \leqslant 2n$ appears in the factorization into primes of the number Q_n. It follows that each of the primes p which does appear in this factorization must be $\leqslant n$, hence, by Lemma 5, it must be $\leqslant \frac{2}{3}n$.

The product of all the different primes p such that $p \mid Q_n$ is, then, not greater than the product of the primes of which none is greater than $\frac{2}{3}n$ hence in virtue of Lemma 2 does not exceed $4^{2n/3}$. By Lemma 3 and the relation $Q_n \mid \binom{2n}{n}$, the exponent of a prime number p in the factorization of the number Q_n into primes can be greater than 1 only in the case where $p < \sqrt{2n}$. The number of such primes is in virtue of Lemma 7 (with $[\sqrt{2n}]$ in place of n — this substitution is justified because, since $n \geqslant 98$, we have $\sqrt{2n} \geqslant 14$) less than $\sqrt{2n}/2$. By Lemma 4 the product of the powers of the primes in question appearing in the factorization into primes of the number $\binom{2n}{n}$ is $< (2n)^{\sqrt{2n}/2}$. We obtain of course the same inequality for the product of the powers of the primes appearing in the factorization into primes of number Q_n. Hence it follows that $Q_n < 4^{2n/3}(2n)^{\sqrt{2n}/2}$. But since $\binom{2n}{n} = Q_n R_n$, in virtue of Lemma 1 we obtain $Q_n R_n > 4^n/2\sqrt{n}$ and thus formula (10) follows. □

LEMMA 9. *For natural numbers $k \geqslant 8$ we have $2^k > 18(k+1)$.*

PROOF. We have $2^8 = 256 > 18 \cdot 9$. If $2^k > 18(k+1)$, then $2^{k+1} = 2^k + 2^k > 18k+18+18k+18 > 18k+36 = 18(k+2)$. Thus, by induction, the lemma follows. □

LEMMA 10. *For real numbers $x \geqslant 8$ we have $2^x > 18x$.*

PROOF. For a real number $x \geqslant 8$ we have $[x] \geqslant 8$. Hence, by Lemma 9, $2^x \geqslant 2^{[x]} > 18([x]+1) > 18x$, whence $2^x > 18x$, as required. □

LEMMA 11. *For natural numbers $k \geqslant 6$ we have $2^k > 6(k+1)$.*

PROOF. In view of Lemma 9 it is sufficient to prove Lemma 11 for $k = 6$ and $k = 7$. To do this we check that $2^6 = 64 > 6 \cdot 7$ and $2^7 = 128 > 6 \cdot 8$. □

LEMMA 12. *For real numbers $x \geqslant 6$ we have $2^x > 6x$.*

The proof is analogous to that of Lemma 10.

LEMMA 13. *If n is a natural number* $\geqslant 648$, *then* $R_n > 2n$.

PROOF. In view of Lemma 8 it is sufficient to prove that if $n \geqslant 648$, then $4^{n/3} > 4n\sqrt{n}\,(2n)^{\sqrt{n/2}}$. To do this we note that, if $n \geqslant 648$, then $\sqrt{2n}/6 > 6$ and, by Lemma 12, $2^{\sqrt{2n}/6} > \sqrt{2n}$, whence, raising each side to the power $\sqrt{2n}$, we obtain $2^{n/3} > (2n)^{\sqrt{n/2}}$. But, since, in virtue of $n \geqslant 648$, we have $2n/9 > 8$, by the use of Lemma 10 we obtain $2^{2n/9} > 4n$, whence $2^{n/3} > 4n\sqrt{4n} > 4n\sqrt{n}$. This, for $n \geqslant 648$, gives $4^{n/3} > 4n\sqrt{n}\,(2n)^{\sqrt{n/2}}$. The lemma is thus proved. □

LEMMA 14. *If* $n \geqslant 648$, *then between n and $2n$ there are at least two different prime numbers.*

PROOF. It follows from the definition of R_n that if there were at most one prime number between n and $2n$, then we should have $R_n \leqslant 2n$, which for $n \geqslant 648$, is impossible because of Lemma 13. □

THEOREM 7. *If n is a natural number* > 5, *then between n and $2n$ there are at least two different prime numbers.*

PROOF. For $n = 6$ the theorem is clearly true, since between 6 and 12 there are two primes, 7 and 11. Thus, in virtue of Lemma 14, the theorem is to be proved for natural numbers n such that $7 \leqslant n < 648$. In order to do this it is not necessary to verify the theorem for each of the natural numbers $7, 8, \ldots, a = 647$ directly. It is sufficient to define a sequence of prime numbers $q_0, q_1, \ldots, q_m$ such that $q_0 = 7$, $q_k < 2q_{k-2}$ for $k = 2, 3, \ldots, m$ and $q_{m-1} > a$. Let n denote an arbitrary natural number such that $7 \leqslant n \leqslant a$. The first term of the sequence $q_0, q_1, \ldots, q_m$ is $\leqslant n$ and the last but one term is $> a \geqslant n$. Thus there exists the greatest index k with $k < m-1$ such that $q_k \leqslant n$. We have $k+2 \leqslant m$, $n < q_{k+1}$ and thus, in virtue of the relation $q_{k+2} < 2q_k \leqslant 2n$, between n and $2n$ there are at least two prime numbers q_{k+1} and q_{k+2}. □

By the use of the tables of prime numbers we can easily check that the sequence defined above is the sequence 7, 11, 13, 19, 23, 37, 43, 73, 83, 139, 163, 277, 317, 547, 631, 653, 1259.

As an immediate corollary to Theorem 7 we derive

THEOREM 8 (Tchebycheff). *If n is a natural number > 3, then between n and $2n-2$ there is at least one prime number.*

PROOF. For $n = 4$ and $m = 5$ the theorem is true, since between 4 and 6 is the prime 5, and between 5 and 8 is the prime 7. If $n > 5$, then, in virtue of theorem 7, between n and $2n$ there are at least two prime numbers. If the greater of them is $q = 2n-1$, then the other must be $< 2n-2$, since $2n-2$, for $n > 5$, is a composite number. We then have $n < p < 2n-2$. If $q < 2n-1$, then, since $p < q$, we obtain also $n < p < 2n-2$. ☐

Theorem 8 was conjectured by J. Bertrand in 1845 and first proved by P. Tchebycheff in 1850. The proof given above is a modification, due to L. Kalmár, of the proof by P. Erdös [1].

COROLLARY 1. *If n is a natural number > 1, then between n and $2n$ there is at least one prime number.*

PROOF. In virtue of Theorem 8 the corollary is true for natural numbers > 3. To verify it for $n = 2$ and $n = 3$ we check that between the numbers 2 and 4 is the prime 3 and between the numbers 3 and 6 is the prime 5. ☐

In 1892 J. J. Sylvester [1] proved the following generalization of Corollary 1:

If $n > k$, then in the sequence $n, n+1, n+2, \ldots, n+k-1$ there exists at least one number which has a prime divisor $> k$. From this Corollary 1 is obtained for $n = k+1$. This generalization was proved also by I. Schur [2] in 1924. A shorter and more elementary proof of it was given by P. Erdös [2] in 1934 (cf. Erdös [12]).

COROLLARY 2. *For natural numbers $k > 1$ we have $p_k < 2^k$.*

PROOF. We have $p_2 = 3 < 2^2$. If, for a natural number k, $p_k < 2^k$, then, using Corollary 1, we see that between 2^k and 2^{k+1} there is at least one prime number, which is of course greater than p_k. Thus we must have $p_{k+1} < 2^{k+1}$ and, by induction, the corollary follows. ☐

We note that Corollary 2 is stronger than inequality (3) of § 9; its proof, however, is much more difficult.

COROLLARY 3. *In the factorization into primes of number* $n!$ *with* $n > 1$ *there is at least one prime factor whose exponent is* 1.

PROOF. For $n = 2$ the corollary is trivially true. If $n = 2k > 1$, where k is a natural number > 1, then, by Corollary 1, there exists a prime number p such that $k < p < 2k$, whence $p < n < 2p$ and consequently p is a divisor of only one of the factors of the product $1 \cdot 2 \cdot \ldots \cdot n$. On the other hand, if $n = 2k+1$, where k is a natural number, then there exists a prime number p such that $k < p < 2k < n$, whence $2k < 2p$ and therefore $2k+1 < 2p$, i.e. $p < n < 2p$, which proves Corollary 3 analogously to the previous case. □.

As an immediate consequence of Corollary 3 we have

COROLLARY 4. *For natural numbers* $n > 1$ *number* $n!$ *is not a k-th power with* $k > 1$ *being a natural number.*

Now, from Theorem 7 we derive

THEOREM 9. *For natural numbers* $k > 3$ *we have* $p_{k+2} < 2p_k$.

PROOF. Let k denote a natural number > 3. We then have $p_k > p_3 = 5$. In virtue of Theorem 7, between p_k and $2p_k$ there are at least two different prime numbers, but, since the least two prime numbers greater than p_k are p_{k+1} and p_{k+2}, we must have $p_{k+2} < 2p_k$ and this is what was to be proved. □

We note that, conversely, Theorem 9 immediately implies Theorem 7. In fact, suppose that Theorem 9 is true. Then if n denotes an arbitrary natural number > 6, i.e. $n \geqslant 7$, we have $p_4 = 7 \leqslant n$. Let p_k be the greatest prime number such that $p_k \leqslant n$. We then have $k > 3$ and $p_{k+1} > n$. Therefore, by Theorem 9, $p_{k+2} < 2p_k \leqslant 2n$. Thus we see that between n and $2n$ there are at least two prime numbers, p_{k+1} and p_{k+2}. Thus all that remains is to verify Theorem 7 for $n = 6$.

We have thus proved that Theorems 7 and 9 are equivalent in the sense that one can easily be deduced from the other.

COROLLARY 1. *We have* $p_{k+1} < 2p_k$ *for* $k = 1, 2, \ldots$

PROOF. For $k = 4, 5, \ldots$ Corollary 1 follows immediately from Theorem 9. We verify Corollary 1 for $k = 1, 2, 3$; $p_2 = 3 < 4 = 2p_1$, $p_3 = 5 < 6 = 2p_2$, $p_4 = 7 < 10 = 2p_3$. ☐

COROLLARY 2. *For natural numbers $k > 1$ we have $p_{k+2} < p_k + p_{k+1}$.*

PROOF. For $k > 3$ the relation follows immediately from Theorem 9; for, $p_{k+2} < 2p_k < p_k + p_{k+1}$ (since $p_k < p_{k+1}$). We verify that it is also true for $k = 2$ and $k = 3$. In fact, $p_4 = 7 < 3+5 = p_2+p_3$ and $p_5 = 11 < 5+7 = p_3+p_4$. ☐

EXERCISES. 1. Find the natural numbers n such that n is the sum of all the primes less than n.

SOLUTION. It is clear that the least possible natural number of this kind is $5 = 2+3$. Suppose, further, that $n > 5$ and that n is the sum of all the prime numbers less than n. If p_k is the greatest prime number less than n, then since $n > 5$, we have $p_k \geqslant 5$. Consequently $k > 2$ and $p_1 + p_2 + \ldots + p_k = n \leqslant p_{k+1}$. Since $k > 2$, Corollary 2 of Theorem 9 gives $p_{k+1} < p_{k-1} + p_k$ and consequently $p_1 + p_2 + \ldots + p_k < p_{k-1} + p_k$, which is clearly impossible. Thus we conclude that only number 5 satisfies the condition of the exercise.

2. Prove that if $n > 1$ and k are natural numbers, then the number $\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{n+k}$ cannot be an integer.

PROOF. If the number in question were an integer we would have $\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{n+k} \geqslant 1$, whence, since $\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{n+k} < \frac{k+1}{n}$, we would obtain $k+1 > n$, and consequently $k \geqslant n$. Let p denote the greatest prime number $\leqslant n+k$. We have $2p > n+k$; for, in view of Corollary 1 of Theorem 8, between p and $2p$ there is a prime q, and for $2p \leqslant n+k$, we would have $p < q < n+k$, contrary to the definition of p. Since $k \geqslant n$, we have $n+k \geqslant 2n$, and, by Corollary 1, there is a prime r between n and $2n$. Hence $r < 2n \leqslant n+k$ and the definition of p implies that $r \leqslant p$. But, since $n < r$, we have $n < p \leqslant n+k < 2p$. It follows that among the summands of the sum $\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{n+k}$ there is only one whose denominator is divisible by the prime p. From this we easily infer that the sum in question cannot be an integer. In fact, reducing the fraction to the same denominator $n(n+1)\ldots(n+k)$, we see that all the numerators but one are divisible by the prime p, this being also a divisor of the denominator. Thus we have proved that none of the partial sums of the harmonic series $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots$ can be an integer provided we do not take into account the trivial case where the sum consists only of the first term. ☐

3. Prove that Corollary 1 of Theorem 8 is equivalent to the following assertion T:

T. *Every finite sequence of consecutive natural numbers which contains at least one prime number contains also at least one number prime to each of the remaining terms of the sequence* (cf. Zahlen [1]).

PROOF. Let

(i) $$k, k+1, \ldots, l$$

be a sequence of consecutive natural numbers and p the greatest of the primes contained in this sequence. If $2p$ were $\leqslant l$, then, according to Corollary 1 of Theorem 8, there would exist a prime number q such that $p < q < 2p \leqslant l$, contrary to the definition of p as the greatest prime number of the sequence (i). Accordingly, we have $l < 2p$. Hence, as can easily be seen, the number p is prime to each of the numbers $1, 2, \ldots, l$ different from p, and consequently, it is of course prime to each term of (i) different from p. We have thus proved that Corollary 1 to Theorem 8 implies theorem T.

Now we suppose that Theorem T holds. Let $n > 1$ be a natural number. According to Theorem T, in the sequence

(ii) $$2, 3, \ldots, 2n,$$

containing the prime 2, there exists at least one number p which is prime to each of the remaining terms of the sequence. First we note that p must be a prime number. In fact, if $p = ab$, where a and b are natural numbers each > 1, then the number $a < p$ belongs to sequence (ii) and is not relatively prime to p. Further, if p were $\leqslant n$, then $2p \leqslant 2n$ and the number $2p \neq p$ would belong to (ii) and $2p$ would not be relatively prime to p. Thus we have $p > n$. But, since p belongs to sequence (ii) $p \leqslant 2n$. Moreover $p \neq 2n$ because $n > 1$ and p is a prime. From this we conclude that $n < p < 2n$. We have thus proved that Theorem T implies Corollary 1 of Theorem 8, which, together with the first part of the proof, shows that Theorem T and Corollary 1 of Theorem 8 are equivalent in the sense that one can easily be deduced from the other. □

4. Using Corollary 1 of Theorem 8 prove that for natural numbers k and $n \geqslant 2^k$ the least k numbers > 1 divisible by none of the numbers $2, 3, \ldots, n$ are primes.

PROOF. If $n \geqslant 2^k$, then $n^2 \geqslant 2^k n$ and, since, in virtue of Corollary 1 of Theorem 8, between any two consecutive terms of the sequence $n, 2n, 2^2 n, \ldots, 2^k n$ there is at least one prime number, between n and n^2 there are at least k different prime numbers. Then of course between n and n^2 there exist at least k numbers not divisible by any of the numbers $2, 3, \ldots, n$. Each of these k numbers is a prime, since, if l is such a number and $l = ab$, where a, b are natural numbers $> 1, a \leqslant b$, then we cannot have $a \leqslant n$ (since l is not divisible by any of the numbers $2, 3, \ldots, n$); thus we must have $b \geqslant a \geqslant n$, whence $l = ab \geqslant n^2$, which is impossible. From this the theorem follows at once. □

11. Theorem of H. F. Scherk

THEOREM 10 (H. F. Scherk). *For every natural number n and a suitable choice of the signs + or − we have*

(11) $$p_{2n} = 1 \pm p_1 \pm p_2 \pm \cdots \pm p_{2n-2} + p_{2n-1}$$

and

$$(12) \qquad p_{2n+1} = 1 \pm p_1 \pm p_2 \pm \cdots \pm p_{2n-1} + 2p_{2n}.$$

These formulae were found by H. F. Scherk [1] in 1830, a proof of H. F. Scherk's formulae was published by S. S. Pillai [1] in 1928. The proof that will be presented here was published by me in 1952 (Sierpiński [14]). A similar proof was published by R. Teuffel [1] in 1955.

PROOF. We say that an infinite sequence $q_1, q_2, \ldots$ has property P if it is an increasing sequence of natural numbers, odd except the first term, such that

$$(13) \quad q_1 = 2,\ q_2 = 3,\ q_3 = 5,\ q_4 = 7,\ q_5 = 11,\ q_6 = 13,\ q_7 = 17$$

and

$$(14) \qquad q_{n+1} < 2q_n \quad \text{for} \quad n = 1, 2, \ldots$$

In particular, in view of Corollary 1 of Theorem 9, the sequence $q_n = p_n$ (for $n = 1, 2, \ldots$) has property P. Accordingly, to prove the theorem of Scherk it is sufficient to prove that for a suitable choice of the signs formulae (11) and (12) are valid for any sequence which has property P.

LEMMA. *If $q_1, q_2, \ldots$ is an infinite sequence having property* P, *then for $n \geqslant 3$ every odd natural number $\leqslant q_{2n+1}$, is of the form $\pm q_1 \pm q_2 \pm \cdots \pm q_{2n-1} + q_{2n}$ provided the signs $+$ or $-$ are suitably chosen.*

PROOF OF THE LEMMA. It follows from (13) that the lemma is true for $n = 3$, since

$1 = -q_1 + q_2 + q_3 - q_4 - q_5 + q_6,$ $\quad 11 = q_1 - q_2 - q_3 - q_4 + q_5 + q_6,$
$3 = q_1 - q_2 - q_3 + q_4 - q_5 + q_6,$ $\quad 13 = q_1 - q_2 + q_3 + q_4 - q_5 + q_6,$
$5 = q_1 + q_2 + q_3 - q_4 - q_5 + q_6,$ $\quad 15 = -q_1 + q_2 + q_3 + q_4 - q_5 + q_6,$
$7 = -q_1 - q_2 - q_3 - q_4 + q_5 + q_6,$ $\quad 17 = q_1 + q_2 - q_3 - q_4 + q_5 + q_6,$
$9 = q_1 + q_2 - q_3 + q_4 - q_5 + q_6,$

We note, that for $n = 2$ the lemma is not true because no choice of the signs $+$ or $-$ would give us $5 = \pm 2 \pm 3 \pm 5 + 7$.

Now suppose that the lemma is true for a natural number $n \geqslant 3$ and let $2k-1$ be an odd natural number $\leqslant q_{2n+3}$. In view od (14) we have $q_{2n+3} < 2q_{2n+2}$ and consequently $-q_{2n+2} < 2k-1-q_{2n+2} < q_{2n+2}$. Therefore for a suitable choice of the signs $+$ or $-$ we have $0 \leqslant \pm(2k-1-q_{2n+2}) < q_{2n+2}$. In virtue of (14), we have $q_{2n+2} < 2q_{2n+1}$ and consequently

$$-q_{2n+1} \leqslant \pm(2k-1-q_{2n+2}) - q_{2n+1} < q_{2n+1},$$

and, moreover, for a suitable choice of the signs + or − we have

$$(15)\qquad 0 \leqslant \pm\{\pm(2k-1-q_{2n+2})-q_{2n+1}\} \leqslant q_{2n+1}.$$

Each of the numbers q_{2n+1} and q_{2n+2} is odd, and so the number in the middle of inequalities (15) is an odd natural number $\leqslant q_{2n+1}$. Consequently, by the use of the inductive assumption, we conclude that for a suitable choice of the signs + or − we have

$$\pm\{\pm(2k-1-q_{2n+2})-q_{2n+1}\} = \pm q_1 \pm q_2 \pm \dots \pm q_{2n-1} + q_{2n}.$$

Hence, if the signs + or − are suitably chosen, we have

$$2k-1 = \pm q_1 \pm q_2 \pm \dots \pm q_{2n} \pm q_{2n+1} + q_{2n+2},$$

which proves the lemma for $n+1$ and at the same time, by induction, for all natural numbers $n \geqslant 3$. □

COROLLARY. *For a suitable choice of the signs + or − we have*

$$(16)\qquad q_{2n+1} = \pm q_1 \pm q_2 \pm \dots \pm q_{2n-1} + q_{2n}.$$

PROOF OF THE COROLLARY. Since q_{2n+1} is an odd natural number, then for $n \geqslant 3$ formula (16) follows immediately from the lemma. For $n = 1$ and $n = 2$ a straightforward computation shows that, in virtue of (13), $q_3 = q_1 + q_2$ and $q_5 = q_1 - q_2 + q_3 + q_4$. □

Now, we are going to prove formulae (11) and (12).

PROOF OF FORMULA (12). For $n \geqslant 3$ the number $q_{2n+1} - q_{2n} - 1$ is, by (14), an odd natural number $< q_{2n+1}$. Therefore, applying the lemma, we see that for a suitable choice of the signs + or − we have $q_{2n+1} - q_{2n} - 1 = \pm q_1 \pm q_2 \pm \dots \pm q_{2n-1} + q_{2n}$, whence (with $q_i = p_i$, $i = 1, 2, \dots$) formula (12) follows. For $n = 1$ and $n = 2$ a straightforward computation shows that $q_3 = 1 - q_1 + 2q_2$, $q_5 = 1 - q_1 + q_2 - q_3 + 2q_4$. Formula (12) is thus proved for all natural numbers n. □

PROOF OF FORMULA (11). In virtue of (14) we have $q_{2n+2} < 2q_{2n+1}$ and we see that $q_{2n+2} - q_{2n+1} - 1$ is an odd natural number > 0 and $< q_{2n+1}$. Now, applying the lemma, we see that for $n \geqslant 3$ and a suitable choice of the signs + or − we have

$$q_{2n+2} - q_{2n+1} - 1 = \pm q_1 \pm q_2 \pm \dots \pm q_{2n-1} + q_{2n},$$

whence

$$(17)\qquad q_{2n+2} = 1 \pm q_1 \pm q_2 \pm \dots \pm q_{2n-1} + q_{2n} + q_{2n+1}.$$

Moreover, by (13), we see that

$$q_2 = 1+q_1, \qquad q_4 = 1-q_1+q_2+q_3,$$
$$q_6 = 1+q_1-q_2-q_3+q_4+q_5,$$

which proves formula (17) for $n = 0, 1$ and 2. Consequently formula (17) is valid for $n = 0, 1, 2, \ldots$ and therefore (for $q_i = p_i$, $i = 1, 2, \ldots$) formula (11) holds for $n = 1, 2, 3, \ldots$ The theorem of Scherk is thus proved. □

12. Theorem of H.-E. Richert

LEMMA 1. *If* $m_1, m_2, \ldots$ *is an infinite increasing sequence of natural numbers such that for a certain natural number* k *the inequality*

$$(18) \qquad m_{i+1} \leqslant 2m_i \quad \textit{for} \quad i > k$$

holds, and if there exist an integer $a \geqslant 0$ *and natural numbers* r *and* $s_{r-1} \geqslant m_{k+r}$ *such that each of the numbers*

$$(19) \qquad a+1, \quad a+2, \quad \ldots, \quad a+s_{r-1}$$

is the sum of different numbers of the sequence $m_1, m_2, \ldots, m_{k+r-1}$, *then for* $s_r = s_{r-1}+m_{k+r}$ *each of the numbers*

$$(20) \qquad a+1, \quad a+2, \quad \ldots, \quad a+s_r$$

is the sum of different numbers of the sequence $m_1, m_2, \ldots, m_{k+r}$ *and, moreover,* $s_r \geqslant m_{k+r+1}$.

PROOF OF LEMMA 1. Suppose that the conditions of the lemma are satisfied. Let n denote a natural number of sequence (20). If $n \leqslant a+s_{r-1}$, then there is nothing to prove, since, by assumption, n is the sum of different terms of the sequence $m_1, m_2, \ldots, m_{k+r-1}$. Suppose then that $n > a+s_{r-1}$. Since $s_{r-1} \geqslant m_{k+r}$, we have $n \geqslant a+1+m_{k+r}$. Consequently $n-m_{k+r} \geqslant a+1$. Moreover, since n is a term of sequence (20), we have $n \leqslant a+s_r = a+s_{r-1}+m_{k+r}$. So $n-m_{k+r} \leqslant a+s_{r-1}$. Therefore the number $n-m_{k+r}$ is a term of sequence (19) and, consequently, it is the sum of different numbers of the sequence $m_1, m_2, \ldots, m_{k+r-1}$. It follows that n is the sum of different numbers of the sequence $m_1, m_2, \ldots, m_{k+r}$. Further, in virtue of (18), we have $m_{k+r+1} \leqslant 2m_{k+r}$, so $s_r = s_{r-1}+m_{k+r} \geqslant 2m_{k+r} \geqslant m_{k+r+1}$. The lemma is thus proved. □

LEMMA 2. *If* $m_1, m_2, \ldots$ *is an infinite sequence of natural numbers such that formula* (18) *holds for a natural number* k *and if there exist an integer* $a \geqslant 0$ *and a natural number* $s_0 \geqslant m_{k+1}$ *such that each of the numbers*

$$(21) \qquad a+1, \quad a+2, \quad \ldots, \quad a+s_0$$

is the sum of different terms of the sequence $m_1, m_2, \ldots, m_k$ *then every natural number* $> a$ *is the sum of different terms of the sequence* $m_1, m_2, \ldots$

PROOF OF LEMMA 2. Suppose that the conditions of the lemma are satisfied. Applying Lemma 1 with $r = 1, 2, \ldots, l$ succesively, l being a natural number, we conclude that each of the numbers

$$(22) \qquad a+1, \quad a+2, \quad \ldots, \quad a+s_l$$

is the sum of different terms of the sequence $m_1, m_2, \ldots, m_{k+l}$. But since $s_r > s_{r-1}, r = 1, 2, \ldots, l$, we see that for every natural number n there exists a natural number l such that $n \leqslant a+s_l$. Consequently, every natural number $n > a$ is one of the numbers of the sequence (22), provided the number l is suitably chosen, accordingly, it is the sum of different terms of the infinite sequence $m_1, m_2, \ldots$ The lemma is thus proved. □

Now, let $m_i = p_i$ with $i = 1, 2, \ldots$ In virtue of Corollary 1 of Theorem 9, the conditions of Lemma 2 are satisfied for $a = 6$, $s_0 = 13$, $k = 5$; this is because $13 = p_6$ and each of the numbers 7, 8, ..., 19 is the sum of different prime numbers $\leqslant p_5$.

In fact, $7 = 2+5$, $8 = 3+5$, $9 = 2+7$, $10 = 3+7$, $11 = 11$, $12 = 5+7$, $13 = 2+11$, $14 = 3+11$, $15 = 2+5+7$, $16 = 5+11$, $17 = 2+3+5+7$, $18 = 7+11$, $19 = 3+5+11$. Of course we do not exclude the trivial sums consisting of one term only: number 11 is not the sum of two or more different primes. As a corollary to Lemma 2 we obtain

THEOREM 11. *Every natural number* > 6 *is a sum of different prime numbers* (Richert [1], [2]).

Now suppose that $m_i = p_{i+1}$. The conditions of Lemma 2 are satisfied for $a = 9$, $s_0 = 19$, $k = 6$, since $19 = p_8 = m_7$ so $s_0 = m_{6+1}$ and, moreover, each of the numbers 10, 11, ..., 28 is the sum of different odd prime numbers $\leqslant m_6 = 19$. In fact, we have $10 = 3+7$, $11 = 11$, $12 = 5+7$, $13 = 13$, $14 = 3+11$, $15 = 3+5+7$, $16 = 5+11$, $17 = 17$, $18 = 5+13$, $19 = 3+5+11$, $20 = 7+13$, $21 = 3+5+13$, $22 = 5+17$, $23 = 3+7+13$, $24 = 11+13$, $25 = 5+7+13$, $26 = 3+5+7+11$, $28 = 3+5+7+13$. Thus we obtain

THEOREM 12. *Every natural number* $\geqslant 10$ *is a sum of different odd prime numbers.*

If we admit also number 2 as a summand of the sums, we get

THEOREM 13. *Every natural number* $\geqslant 12$ *is a sum of two or more different prime numbers.*

As can easily be seen, number 11 is not a sum of two or more different prime numbers. Number 17 is not a sum of two or three different prime numbers (but $17 = 2+3+5+7$). One can also prove, using elementary methods only, that there exist infinitely many odd numbers which are not the sums of less than three prime numbers.

Here are four theorems due to R. Dressler, A. Mąkowski and T. Parker [1]:

Every natural number > 1969 *is a sum of different prime numbers of the form* $12k+1$.

Every natural number > 1349 *is a sum of different prime numbers of the form* $12k+5$.

Every natural number > 1387 *is a sum of different prime numbers of the form* $12k+7$.

Every natural number > 1475 *is a sum of different prime numbers of the form* $12k+11$.

The lower bounds given in the theorems are sharp, i.e. cannot be replaced by still lower ones..For some related results see J.L. Brown Jr. [2].

13. A conjecture on prime numbers

Several years ago I formulated the following Conjecture P.

CONJECTURE P. *If the numbers* $1, 2, 3, \ldots, n^2$ *with* $n > 1$ *are arranged in n rows each containing n numbers*:

$$\begin{array}{ccccc} 1, & 2, & 3, & \ldots, & n \\ n+1, & n+2, & n+3, & \ldots, & 2n \\ 2n+1, & 2n+2, & 2n+3, & \ldots, & 3n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (n-1)n+1, & (n-1)n+2, & & \ldots, & n^2 \end{array} \tag{23}$$

then each row contains at least one prime number (Schinzel et Sierpiński [3]).

The first row of table (23) contains of course ($n > 1$) number 2. The assertion that for $n > 1$ the second row contains at least one prime number is another formulation of Corollary 1 to Theorem 8. It easily follows from the inequality of J. B. Rosser and L. Schoenfeld (cf. § 15) that for $n > e^k$ each of the first k rows contains a prime.

As can be verified on the basis of the tables of Lander and Parkin [3] and Brent [1], [4] Conjecture P is true for $1 < n \leqslant 21 \cdot 10^5$. Since the last two rows of table (23) consist of numbers $(n-1)^2, (n-1)^2+1, \ldots, n^2$, Conjecture P implies that between two consecutive squares of natural numbers there are at least two prime numbers. Further, since in every interval whose end-points are cubes of two consecutive natural numbers there are two squares of two consecutive natural numbers, we see that Conjecture P implies that between the cubes of any two consecutive natural numbers there are at least two prime numbers. The last statement has not been proved yet, but it follows from the results of A. E. Ingham of 1937 that the number of primes between n^3 and $(n+1)^3$ tends to infinity with n.

As an immediate consequence of Conjecture P we obtain the assertion that between any two triangular numbers there is at least one prime number. Namely, if we arrange natural numbers in rows in such a manner that in the nth row we put n consecutive natural numbers, i.e. if we form the table

$$\begin{array}{lllll}
1 & & & & \\
2, & 3 & & & \\
4, & 5, & 6 & & \\
7, & 8, & 9, & 10 & \\
11, & 12, & 13, & 14, & 15 \\
\multicolumn{5}{l}{\dots\dots\dots\dots\dots}
\end{array}$$

then each but the first of its rows contains a prime number. We do not know whether the above statement is true.

In 1932 R. Haussner [1] formulated a conjecture that, *for a natural number k, between two consecutive multiples of the prime number p_k both less than p_{k+1}^2 there is at least one prime number.* This conjecture was verified by Haussner for prime numbers $p_k < 100$. Conjecture P for a prime n is an immediate consequence of the conjecture of Haussner. As has been noticed by L. Skula, Conjecture P implies that for every natural number $n > 1$ also $(n+1)$-th row and $(n+2)$-th row of table (23) contain at least one prime number each.

In fact, it follows from Conjecture P for the number $n+1$ that among the numbers $n^2-1, n^2, \ldots, n(n+1)$ there is at least one prime number and, since for $n > 2$ the first two terms of the sequence are composite numbers, at least one prime number is to be found among the numbers $n^2+1, n^2+2, \ldots, (n+1)n$. (This of course is also true for $n = 2$.) It follows from Conjecture P for the number $n+1$ that among the numbers $n^2+n+1, n^2+n+2, \ldots, (n+1)^2$ there is at least one prime number; thus, clearly, there is at least one prime number among the numbers $n^2+n-1, n^2+n, \ldots, n^2+2n$ (since the number $(n+1)^2$ is composite).

With reference to table (23) it should be mentioned that A. Schinzel has formulated a conjecture that, *if n is a natural number > 1 and k a natural number less than n and relatively prime to n, then in the k-th column of table* (23) *there is at least one prime number.* (Schinzel and Sierpiński [3]). In other words, if k and n are natural numbers relatively prime and $k < n$, then among the numbers

$$k, k+n, k+2n, \ldots, k+(n-1)n$$

there is at least one prime number. It follows from the tables of Wagstaff [2] that this holds for all natural numbers $n \leqslant 50000$.

It is necessary to note here that Yu. V. Linnik proved in 1947 the existence of a constant C such that if $(k, n) = 1$ and $1 \leqslant k < n$ the least prime number in the arithmetical progression $k, k+n, k+2n, \ldots$ is less than n^C.

J. R. Chen [3] has proved that on replacing n^C by An^C for a suitable A one can take $C = 17$ (cf. also S. Graham [1], where Chen's new result $C = 14$ is announced).

As observed by A. Schinzel [13], a conjecture somewhat stronger than Conjecture P can be formulated. Namely, one can conjecture that, if x is a real number $\geqslant 117$, then between x and $x+\sqrt{x}$ there is at least one prime number. This Conjecture, P_1, follows from Lander and Parkin's and Brent's tables for $117 \leqslant x \leqslant 4{,}44 \cdot 10^{12}$. It was Legendre who formulated the conjecture that for sufficiently large numbers x there is at least one prime number between x and $x+\sqrt{x}$.

We now show how Conjecture P for $n \geqslant 117$ is derived from Conjecture P_1. Let n denote a natural number $\geqslant 117$ and let k be a natural number less than n. We have $kn \geqslant 117$ and so, by Conjecture P_1, there exists a prime number p such that $kn < p < kn+\sqrt{kn}$. But, since $k < n$, we have $\sqrt{kn} < n$; consequently there exists at least one prime number among the terms of the sequence $kn+1, kn+2, \ldots, (k+1)n$. Since this is valid for every natural number $k < n$, we see that (for $n \geqslant 117$) in each row of table (23) from the second onwards there is at least one prime number. (In the first row, however, for $n > 1$ at least the prime 2 occurs.) Thus we see that Conjecture P for $n \geqslant 117$ follows from Conjecture P_1. For $n < 117$ Conjecture P has been proved by a straightforward verification.

As observed by A. Schinzel [13] a still stronger conjecture than P_1 can be formulated, namely that for each real number $x \geqslant 8$ between x and $x+(\log x)^2$ at least one prime number occurs. Lander and Parkin's and Brent's tables confirm the truth of this conjecture for all $x < 4.44 \cdot 10^{12}$.
If we set $x = p_n$ with $n > 4$, then we obtain the inequality $p_{n+1}-p_n < (\log p_n)^2$ for all $n > 4$. It was H. Cramér [1] who conjectured that $\overline{\lim}\,(p_{n+1}-p_n)/(\log p_n)^2 = 1$.

There is another conjecture about the difference of two consecutive prime numbers, namely the following conjecture of N. L. Gilbreath formulated in 1958. We form a table of natural numbers in this manner: in the first row we write the differences of consecutive prime numbers (i.e. the numbers $p_{n+1}-p_n$, $n = 1, 2, \ldots$), in the second row we write the moduli of the differences of the consecutive numbers of the first row. In each of the following rows we write the moduli of the differences of the consecutive terms of the preceding row. The conjecture of Gilbreath is that the first term of each row is equal to 1.

Here are the initial terms of the first 10 rows obtained in this way:

$$\begin{array}{c}
1,\ 2,\ 2,\ 4,\ 2,\ 4,\ 2,\ 4,\ 6,\ 2 \\
1,\ 0,\ 2,\ 2,\ 2,\ 2,\ 2,\ 2,\ 4 \\
1,\ 2,\ 0,\ 0,\ 0,\ 0,\ 0,\ 2 \\
1,\ 2,\ 0,\ 0,\ 0,\ 0,\ 2 \\
1,\ 2,\ 0,\ 0,\ 0,\ 2 \\
1,\ 2,\ 0,\ 0,\ 2 \\
1,\ 2,\ 0,\ 2 \\
1,\ 2,\ 2 \\
1,\ 0 \\
1
\end{array}$$

The conjecture of Gilbreath has been verified for the first 63418 rows with the aid of the electronic computer SWAC. In general it has not been proved as yet (cf. Killgrove and Ralston [1]).

14. Inequalities for the function $\pi(x)$

Now we are going to deduce some corollaries from Lemma 9 of § 10. Since R_n denotes the product of prime numbers p such that $n < p < 2n$ and the number of such primes is $\pi(2n)-\pi(n)$ (and by Corollary 1 of Theorem 8, §10, for every natural number n at least one such prime p exists) and, moreover, each of those primes is less than $2n$, then $R_n \leqslant (2n)^{\pi(2n)-\pi(n)}$. It follows from formula (10) of § 10 that for natural numbers $n \geqslant 98$ we have

$$(2n)^{\pi(2n)-\pi(n)} > \frac{4^{n/3}}{2\sqrt{n}\,(2n)^{\sqrt{n/2}}};$$

taking the logarithm of each side of the last inequality, we conclude that for $n \geqslant 98$

$$\pi(2n)-\pi(n) > \frac{n}{3\log 2n}\left(\log 4 - \frac{3\log 4n}{2n} - \frac{3\log 2n}{\sqrt{2n}}\right) \tag{24}$$

holds. But, as we know,

$$\lim_{x\to\infty}\frac{\log x}{x} = 0;$$

therefore

$$\lim_{n\to\infty}\bigl(\pi(2n)-\pi(n)\bigr) = +\infty.$$

It follows that for every natural number k there exists a natural number m_k such that for $n \geqslant m_k$ there are at least k prime numbers between n and $2n$.

Further, since $\log x/x$ is, for $x > e$, a decreasing function of x, we have for $n \geqslant 2500$

$$\frac{3\log 4n}{2n} + \frac{3\log 2n}{\sqrt{2n}} = 6\left(\frac{\log 4n}{4n} + \frac{\log\sqrt{2n}}{\sqrt{2n}}\right)$$
$$\leqslant 6\left(\frac{\log 4\cdot 2500}{4\cdot 2500} + \frac{\log\sqrt{2\cdot 2500}}{\sqrt{2\cdot 2500}}\right) < 0{,}37;$$

hence

$$\log 4 - \frac{3\log 4n}{2n} - \frac{3\log 2n}{\sqrt{2n}} > 1{,}38 - 0{,}37 > 1. \tag{25}$$

In virtue of (24), formula (25) gives the inequality of Finsler,

$$\pi(2n)-\pi(n) > \frac{n}{3\log 2n}, \tag{26}$$

which holds not only for $n \geqslant 2500$ but, as can easily be verified, for all natural numbers $n > 1$.

It is even easier to obtain the second inequality of Finsler. We note that for natural numbers n we have $\binom{2n}{n} < 4^n$ (this follows immediately from the binomial formula applied to $(1+1)^{2n} > \binom{2n}{n}$). In view of the relation $R_n \mid \binom{2n}{n}$ we see that $R_n < 4^n$ and from the definition of the number R_n we infer that $R_n \geqslant n^{\pi(2n)-\pi(n)}$. Consequently, $n^{\pi(2n)-\pi(n)} < 4^n$ and hence

$$\pi(2n)-\pi(n) < \frac{n\log 4}{\log n} < \frac{7n}{5\log n}$$

since, as can easily be verified, $\log 4 < \frac{7}{5}$. From this, using (26), we get (cf. Finsler [1] and Trost [3], Satz 32)

$$\frac{n}{3\log 2n} < \pi(2n)-\pi(n) < \frac{7n}{5\log n} \quad \text{for} \quad n > 1. \tag{27}$$

It follows from (27) that

$$\pi(2n) > \frac{n}{3\log 2n} \quad \text{for} \quad n > 1$$

and, since for $n \geqslant 4$ we have $n > n/2 \geqslant [n/2] > n/2-1 > n/4$, and since $\log(2[n/2]) \leqslant \log n$, we see that

$$\pi(n) \geqslant \pi\left(2\left[\frac{n}{2}\right]\right) > \frac{[n/2]}{3\log 2[n/2]} > \frac{n}{12\log n} \quad \text{for} \quad n \geqslant 4,$$

$$\pi(n) > \frac{n}{12\log n} \quad \text{for} \quad n > 1; \tag{28}$$

for, as can easily be verified, the inequality holds for $n = 2$ and $n = 3$ as well.

We are going to prove that

$$\pi(2^k) < \frac{2^{k+1}}{k\log 2} \quad \text{holds for natural numbers } k. \tag{29}$$

As can easily be seen, formula (29) holds for natural numbers $k \leqslant 6$ because $\log 2 < 1$. Now suppose it is valid for a natural number $k \geqslant 6$. In virtue of (27) (with 2^k in place of n) and formula (29) we have

$$\pi(2^{k+1}) < \pi(2^k) + \frac{7 \cdot 2^k}{5k \log 2} < \frac{2^{k+1}}{k \log 2}\left(1 + \frac{7}{10}\right).$$

But, since for $k \geqslant 6$ we have $(k+1)(1+\frac{7}{10}) < 2k$,

$$\pi(2^{k+1}) < \frac{2^{k+2}}{(k+1)\log 2}$$

and thus by induction inequality (29) follows.

Now let n denote a natural number > 1. There exists a natural number k such that $2^k \leqslant n < 2^{k+1}$, whence $(k+1)\log 2 > \log n$. Hence, by (29), we have

$$\pi(n) \leqslant \pi(2^{k+1}) < \frac{2^{k+2}}{(k+1)\log 2} < \frac{4n}{\log n}.$$

From this we see that

$$\pi(n) < \frac{4n}{\log n} \quad \text{for the natural numbers } n > 1. \tag{30}$$

By replacing n by p_n in (28) and (30) and by the fact that $\pi(p_n) = n$ we obtain

$$\frac{p_n}{12 \log p_n} < n < \frac{4p_n}{\log p_n};$$

consequently, since $p_n > n$ (for $n = 1, 2, \ldots$), we infer that

$$p_n > \frac{n}{4} \log p_n > \frac{n \log n}{4} \quad \text{and} \quad p_n < 12n \log p_n,$$

whence $\log p_n < \log 12 + \log n + \log\log p_n$. But, in virtue of Corollary 2 to Theorem 8 of § 10, we see that $p_n < 2^n$, whence $\log p_n < n \log 2$ and $\log\log p_n < \log n + \log\log 2$. Since $\log 2 < 1$, for $n \geqslant 12$ we have $n > 12 \log 2$ and hence $\log n > \log 12 + \log\log 2$. Therefore, for $n \geqslant 12$, we have $\log p_n < 2 \log n + \log 12 + \log\log 2 < 3 \log n$. Consequently, $p_n < 36n \log n$ for all $n \geqslant 12$ and, as is easy to verify, also for $2 \leqslant n < 12$.

Thus we arrive at the final conclusion that

$$\frac{n \log n}{4} < p_n < 36n \log n \quad \text{for} \quad n > 1. \tag{31}$$

From formula (28) we derive the following corollary:

For every natural number s there exists a natural number which can be represented as the sum of two prime numbers in more than s different ways.

PROOF. Suppose that for a natural number s there is no natural number which can be represented as the sum of two prime numbers in more than s ways. Let n denote a natural number > 1. Let us consider all the pairs (p, q) where p, q are prime numbers, neither of them greater than n. The number of such pairs is clearly $[\pi(n)]^2$. We divide the set of the pairs (p, q) into classes by saying that (p, q) belongs to the kth class if $p+q = k$. Since $p \leqslant n$ and $q \leqslant n$, we have $k \leqslant 2n$. By assumption, for a given $k \leqslant 2n$ in the kth class there are at most s different pairs. Since the numbers of all the classes is less than $2n$, the number of the pairs (p, q) is less than $2ns$. Consequently, $[\pi(n)]^2 < 2ns$ and since, by formulae (28), $[\pi(n)]^2 > n^2/12^2(\log n)^2$, we have $2 \cdot 12^2 s(\log n)^2 > n$. But, as is known, $e^x > x^3/3!$ for all $x \geqslant 0$, whence, for $x = \log n$, we have $6n > (\log n)^3$. Therefore $12^3 s(\log n)^2 > (\log n)^3$ for $n > 1$, whence $\log n < 12^3 s$ for all $n > 1$, which for sufficiently large n is not true. Consequently the assumption that for a natural number s there is no natural number which can be represented as the sum of two prime numbers in more than s ways leads to a contradiction. The corollary is thus proved. The conjecture has been formulated that the number of all possible decompositions into the sum of two primes of an even natural number increases with n to infinity. □

REMARK. Numbers which can be represented as sums of two primes in more than one way must be even provided we do not regard two representations as being different if they differ only in the order of the summands. In fact, if an odd number n is the sum of two primes, then of course one of them must be even, i.e. equal to 2, and consequently the other is $n-2$ and we see that the representation of n as the sum of two primes is unique apart from the order of the summands.

By a slight modification of the proof of Corollary 1 one can prove that for every natural number s there exists a natural number which can be represented as the sum of three squares of prime numbers in more than s different ways. P. Erdös [4] has proved that for each natural number s there exists a natural number which is representable as the sum (resp. as the difference) of the squares of two primes in more than s different ways.

It follows immediately from (30) that

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0.$$

$\log n + \log\log n - \log 4 < \log p_n < \log n + \log\log n + \log 36$. Hence immediately

$$\lim_{n\to\infty} \frac{\log p_n}{\log n} = 1. \tag{32}$$

Now we are going to derive a corollary from inequality (31). In virtue of (31) we have

$$\frac{1}{p_k} > \frac{1}{36k\log k} \quad \text{for} \quad k = 2, 3, \ldots,$$

whence for natural numbers $n > 2$ we deduce that

$$\sum_{k=2}^{n} \frac{1}{p_k} > \frac{1}{36} \sum_{k=2}^{n} \frac{1}{k\log k}.$$

But, as we know, $\log(1+x) < x$ for $0 < x < 1$, whence, for $k = 2, 3, \ldots$,

$$\log(k+1) - \log k = \log\left(1 + \frac{1}{k}\right) < \frac{1}{k},$$

consequently,

$$\frac{\log(k+1)}{\log k} < 1 + \frac{1}{k\log k}$$

and

$$\log\log(k+1) - \log\log k$$
$$= \log\frac{\log(k+1)}{\log k} < \log\left(1 + \frac{1}{k\log k}\right) < \frac{1}{k\log k}.$$

Thus we have

$$\frac{1}{k\log k} > \log\log(k+1) - \log\log k \quad \text{for} \quad k = 2, 3, \ldots, n.$$

Hence (for natural $n > 2$) we have

$$\sum_{k=2}^{n} \frac{1}{k\log k} > \log\log(n+1) - \log\log 2 > \log\log(n+1)$$

(since $\log\log 2 < 0$).

We then have

$$\sum_{k=2}^{n} \frac{1}{p_k} > \frac{1}{36} \log\log(n+1).$$

From this we see that the series of the reciprocals of the consecutive prime numbers, i.e. the series

$$\tfrac{1}{2} + \tfrac{1}{3} + \tfrac{1}{5} + \tfrac{1}{7} + \tfrac{1}{11} + \tfrac{1}{13} + \ldots,$$

is divergent.

15. The prime number theorem and its consequences

It follows from formulae (28) and (30) of § 14 that there exist positive numbers (e.g. $a = \frac{1}{12}$, $b = 4$) such that

$$a < \pi(n) : \frac{n}{\log n} < b$$

for natural numbers $n > 1$.

In 1896 J. Hadamard and Ch. de la Vallée Poussin proved that

$$\lim_{x \to \infty} \left(\pi(x) : \frac{x}{\log x} \right) = 1. \tag{33}$$

Nowadays owing to the new methods created by A. Selberg [1] and P. Erdös [9], this formula, known under the name of the *prime number theorem*, can be proved "elementarily", though the proof is very complicated. We will not present it here (¹). If $\pi(n) : \frac{n}{\log n} = h(n)$, then e.g. $h(10^3) = 1.159$, $h(10^4) = 1.132$, $h(10^5) = 1.104$, $h(10^6) = 1.084$, $h(10^7) = 1.071$, $h(10^8) = 1.061$, $h(10^9) = 1.053$, $h(10^{10}) = 1.048$.

A better approximation for the function $\pi(x)$ is obtained by the function

$$\int_0^x \frac{dt}{\log t}$$

(¹) Cf. e.g. Trost [3], Chapter VII: *Elementarer Beweis des Primzahlsatzes*, pp. 66–73: see also LeVeque [1], vol. II, p. 229–263, chapter 7: *The prime number theorem.*

J. E. Littlewood has proved that the difference $\pi(x)-\int\limits_0^x \frac{dt}{\log t}$ takes infinitely many positive values and infinitely many negative values for x running over all natural numbers.

Proofs of the theorem of Littlewood and of the other theorems mentioned in this chapter, which require analytical methods, can be found in the book of K. Prachar [1].

In formula (33) setting $x = p_n$, by $\pi(p_n) = n$ we obtain

$$\lim_{n\to\infty} \frac{n\log p_n}{p_n} = 1,$$

whence, by (32), we get

$$\lim_{n\to\infty} \frac{p_n}{n\log n} = 1, \tag{34}$$

and consequently we see that an approximate value for p_n is the number $n \log n$, provided n is sufficiently large.

It follows immediately from (34) that

$$\lim_{n\to\infty} \frac{p_{n+1}}{p_n} = 1.$$

J. B. Rosser [1] has proved that for all natural numbers n the inequality $p_n > n\log n$ holds.

More information about $\pi(n)$ than that can be derived from formula (33) is given by the theorem of J. B. Rosser and L. Schoenfeld [1] stating that

$$\frac{n}{\log n-\frac{1}{2}} < \pi(n) < \frac{n}{\log n-\frac{3}{2}} \tag{35}$$

for every natural number $n \geqslant 67$.

Clearly formula (33) follows at once from (35).

But even from inequality (35) we are unable to derive certain simple properties of the function $\pi(n)$. For example such is the case with the theorem of E. Landau (cf. Landau [3], vol. I, pp. 215–216) stating that $\pi(2n) < 2\pi(n)$ holds for sufficiently large numbers n, which means that there are more prime numbers in the interval $0 < x \leqslant n$ than there are in the interval $n < x \leqslant 2n$, provided n is large enough. According to Rosser and Schoenfeld [2] it suffices to assume $n \geqslant 11$. In this connection we may ask whether for natural numbers $x > 1$ and $y > 1$ the inequality

$$\pi(x+y) \leqslant \pi(x)+\pi(y) \tag{36}$$

holds. This, clearly, would imply that the inequality $\pi(2n) \leqslant 2\pi(n)$ is valid for any natural n. Inequality (36) has been proved by A. Schinzel [13] for $\min(x, y) \leqslant 146$, by J. L. Selfridge much further on (unpublished) and has been verified by S. L. Segal [1] for $x+y \leqslant 100000$. However, D. Hensley and I. Richards [1] have proved that (36) is incompatible with the hypothesis H. Using their method T. Vehka [1] has recently shown that incompatibility occurs already for $\min(x, y) = 11763$. With reference to the function $\pi(x)$ we note that the function assigning to a pair of natural numbers k and x the number of positive integers $\leqslant x$ having precisely k prime divisors, resp. k natural divisors, has also been investigated and the formulae describing its asymptotic behaviour have been found (cf. Sathe [1], Selberg [2], resp. LeVeque [1]).

Now let a and b be two real numbers such that $0 < a < b$. Since, as can easily be seen, $\lim\limits_{x\to\infty} \dfrac{\log ax}{\log bx} = 1$, by (33), we have

$$\lim_{x\to\infty} \frac{\pi(bx)}{\pi(ax)} = \frac{b}{a}.$$

Consequently, since $0 < a < b$, $\pi(bx) > \pi(ax)$, provided n is large enough. This proves the following assertion:

If a and b are two positive real numbers and $a < b$, then for sufficiently large real numbers x there is at least one prime number between ax and bx.

In particular, if $a = 1$ and $b = 1+\varepsilon$ where ε is an arbitrary positive real number, it follows that there is at least one prime number between n and $n(1+\varepsilon)$ provided n is large enough.

Now let $c_1, c_2, \ldots, c_m$ be an arbitrary finite sequence consisting of digits. Let a be the number whose digits are $c_1, c_2, \ldots, c_m$. Applying the corollary just derived from formula (33) we see that $\pi(an) < (\pi(a+1)n)$ holds for sufficiently large numbers n. Consequently, there exists a natural number s such that $\pi(a\cdot 10^s) < \pi((a+1)\cdot 10^s)$. Therefore there exists a prime number p such that $a\cdot 10^s < p < (a+1)\cdot 10^s$.

Thus the first m digits of the number p are identical with the corresponding digits of the number a. This means that the first m digits of the number p are $c_1, c_2, \ldots, c_m$. Thus, as another consequence of formula (33), we obtain the following corollary:

For an arbitrary finite sequence $c_1, c_2, \ldots, c_m$ *of digits there exists a primenumber whose first m digits are* $c_1, c_2, \ldots, c_m$ (¹).

Let x denote a real number > 0. For sufficiently large natural numbers n we have $nx > 2$; so $\pi(nx) \geqslant 1$. It follows from (34) that

$$\lim_{n\to\infty} \frac{p_{\pi(nx)}}{\pi(nx)\log\pi(nx)} = 1. \tag{37}$$

But, in virtue of (33), we have

$$\lim_{n\to\infty} \frac{\pi(nx)\log nx}{nx} = 1, \tag{38}$$

whence $\lim\limits_{n\to\infty} (\log\pi(nx) + \log\log nx - \log nx) = 0$, which proves that

$$\lim_{n\to\infty} \frac{\log\pi(nx)}{\log nx} = 1. \tag{39}$$

From formulae (37), (38) and (39) we infer that

$$\lim_{n\to\infty} \frac{p_{\pi(nx)}}{nx} = 1.$$

We have thus proved that formula (33) implies the fact, observed by H. Steinhaus, that for every real number $x > 0$ there exists an infinite sequence of prime numbers $q_1, q_2, \ldots$ such that

$$\lim_{n\to\infty} \frac{q_n}{n} = x.$$

Finally, let a and b be two arbitrary real numbers such that $a < b$. It follows from the above corollary to formula (33) that, if q is a sufficiently large prime number,then there exists a prime number p such that $aq < p < bq$, whence $a < p/q < b$.

This proves that the set of the quotients p/q, p and q being prime numbers, is dense in the set of positive real numbers.

(¹) Cf. Sierpiński [10] and Trost [3], p. 42 (Theorem 20), see also Sierpiński [25]. There a stronger theorem is proved.

CHAPTER IV

NUMBER OF DIVISORS AND THEIR SUM

1. Number of divisors

The number of the divisors of a given natural number n is denoted by $d(n)$. In order to establish the table of the function $d(n)$ one may use the following method which is a modification of the sieve of Eratosthenes. In order to find the values $d(n)$ for $n \leqslant a$ we write down the natural numbers $1, 2, \ldots, a$ and we mark all of them. Next we mark those which are divisible by 2, then those which are divisible by 3, and so on. Finally we mark only the number a. The number of the divisors of a number n is equal to the number of the marks on it (cf. Harris [1]). In particular, for $a = 20$ we have

$$\underline{1},\ \underline{\underline{2}},\ \underline{\underline{3}},\ \underline{\underline{\underline{4}}},\ \underline{\underline{5}},\ \underline{\underline{\underline{\underline{6}}}},\ \underline{\underline{7}},\ \underline{\underline{\underline{\underline{8}}}},\ \underline{\underline{\underline{9}}},\ \underline{\underline{\underline{\underline{10}}}},\ \underline{\underline{11}},\ \underline{\underline{\underline{\underline{\underline{\underline{12}}}}}},\ \underline{\underline{13}},\ \underline{\underline{\underline{\underline{14}}}},\ \underline{\underline{\underline{\underline{15}}}},\ \underline{\underline{\underline{\underline{\underline{16}}}}},\ \underline{\underline{17}},\ \underline{\underline{\underline{\underline{\underline{\underline{18}}}}}},\ \underline{\underline{19}},\ \underline{\underline{\underline{\underline{\underline{\underline{20}}}}}}.$$

Hence we find $d(1) = 1$, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$, $d(5) = 2$, $d(6) = 4$, $d(7) = 2$, $d(8) = 4$, $d(9) = 3$, $d(10) = 4$, $d(11) = 2$, $d(12) = 6$, $d(13) = 2$, $d(14) = 4$, $d(15) = 4$, $d(16) = 5$, $d(17) = 2$, $d(18) = 6$, $d(19) = 2$, $d(20) = 6$.

Let n be a natural number greater than 1 and let

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k} \tag{1}$$

be the factorization of n into prime numbers. Suppose that d is a divisor of n. Since every divisor of d is a divisor of n, then in the factorization of the number d into primes only the primes appearing in (1) can possibly appear and, moreover, the exponents of them cannot be greater than those of the corresponding primes in (1). Accordingly, every divisor d of the number n can be written in the form

$$d = q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k}, \tag{2}$$

where λ_i $(i = 1, 2, \ldots, k)$ are integers satisfying the inequalities

$$0 \leqslant \lambda_i \leqslant \alpha_i \quad \text{for} \quad i = 1, 2, \ldots, k. \tag{3}$$

On the other hand, it is obvious that every number that can be written in form (2), numbers λ_i satisfying inequalities (3), is a natural divisor of the number n. This is because, in view of (3), $n/d = q_1^{\alpha_1-\lambda_1} q_2^{\alpha_2-\lambda_2} \ldots q_k^{\alpha_k-\lambda_k}$ is an integer.

Finally, it is obvious that different systems of integers

$$\lambda_1, \lambda_2, \ldots, \lambda_k \tag{4}$$

satisfying (3) define different numbers (2). We have thus proved the following

THEOREM 1. *If n is a natural number whose factorization into prime numbers is written as* (1), *then taking for the numbers in* (4) *all the different systems of k integers which satisfy inequalities* (3) *we find that all the divisors of the number n are given by* (2). *Moreover, to each system corresponds precisely one divisor.*

Consequently, the number of divisors of a natural number n whose factorization into prime numbers is written as (1) is equal to the number of all the systems of integers (4) satisfying inequalities (3). It is a matter of simple computation to calculate the number of the systems. In fact, in order that an integer λ_i should satisfy inequalities (3) it is necessary and sufficient that λ_i should belong to the sequence

$$0, 1, 2, \ldots, \alpha_i.$$

Thus for a given $i = 1, 2, \ldots, k$ the number λ_i can take $\alpha_i + 1$ different values. This proves

THEOREM 2. *The number $d(n)$ of the divisors of a natural number n whose factorization into primes is written as* (1) *is given by*

$$d(n) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1). \tag{5}$$

Let us calculate the number $d(60)$ for instance. We have $60 = 2^2 \cdot 3 \cdot 5$. Therefore, in view of (5), $d(60) = (2+1)(1+1)(1+1) = 12$. Similarly, since $100 = 2^2 \cdot 5^2$, we see that $d(100) = (2+1)(2+1) = 9$.

It follows from (5) that for every natural number $s > 1$ there exist infinitely many natural numbers which have precisely s divisors. In fact, if $n = p^{s-1}$, where p is a prime, then $d(n) = d(p^{s-1}) = s$.

Clearly, the equality $d(n) = 1$ implies $n = 1$. Formula (5) shows that $d(n) = 2$ whenever $k = 1$ and $\alpha_1 = 1$, that is, whenever n is a prime. Accordingly, the solutions of the equation $d(n) = 2$ are prime numbers. Consequently, for composite numbers n we have $d(n) \geqslant 3$.

It follows from (5) that $d(n)$ is an odd number if and only if all the α_i's ($i = 1, 2, \ldots, k$) are even, that is, if and only if n is the square of a natural number.

EXERCISES. 1. Prove that for natural numbers n we have $d(n) \leqslant 2\sqrt{n}$.

The proof follows from the fact that of two complementary divisors of a natural number n one is always not greater than $\sqrt{n}$.

2. Find all the natural numbers which have precisely 10 divisors.

SOLUTION. If $d(n) = 10$, then, in view of (5), we have $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1) = 10$. We may, of course, assume that $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_k$. Since there are two ways of presenting 10 as the product of natural numbers > 1 written in the order of their magnitude, namely $10 = 2\cdot 5$ and $10 = 10$, then either $k = 2, \alpha_1 = 1, \alpha_2 = 4$, or $k = 1, \alpha_1 = 9$. It follows that the natural numbers which have precisely 10 divisors are either the numbers $p\cdot q^4$, where $p, q \neq p$ are arbitrary primes, or the numbers p^9, where p is an arbitrary prime.

3. Find the least natural number n for which $d(n) = 10$.

SOLUTION. In view of Exercise 2 and the fact that of the numbers 2^9, $2\cdot 3^4$, and $3\cdot 2^4$ the latter is least, it follows that the least natural number n for which $d(n) = 10$ is the number $n = 3\cdot 2^4 = 48$.

REMARK. In general it is easy to prove that for given prime numbers p, q with $q > p$ the least natural number that has precisely pq divisors is the number $2^{q-1}\cdot 3^{p-1}$.

4. Prove that, if n is a natural number > 1, then in the infinite sequence

$$n,\ d(n),\ d\big(d(n)\big),\ ddd(n), \ldots$$

all the terms starting from a certain place onwards are equal to 2. Prove that the place can be arbitrarily given.

The proof follows immediately from the remark that if n is a natural number greater than 2, then $d(n) < n$, and from the equality $d(2) = 2$. To prove the second part of the exercise we use the equality $d(2^{n-1}) = n$.

5. Prove that for any natural number m the set of the natural numbers n such that the number of the divisors of n is divisible by m contains an infinite arithmetical progression.

PROOF. We note that the numbers $2^m t + 2^{m-1}$ ($t = 0, 1, 2, \ldots$) form an infinite arithmetical progression and belong to the set defined above for the number m. In fact, the exponent of the number 2 in the factorization of the number $n = 2^m t + 2^{m-1}$ is $m-1$. Hence, by (1), we see that $m \mid d(n)$. ☐

REMARK. As an immediate consequence of the theorem proved above we obtain that for any natural number m the set of natural numbers n such that $m \mid d(n)$ has positive lower density. This means that there exists a positive number a with the property that the number $S_m(x)$ of the natural numbers $n \leqslant x$ for which $m \mid d(n)$ is greater than ax for all x large enough. E. Cohen [1] proved that for any natural number m the limit $\lim\limits_{x\to\infty} \dfrac{S_m(x)}{x}$ exists and is positive.

In the year 1940 the tables of the function $d(n)$ for $n \leqslant 10000$ were published, cf. Glaisher [2]. As we check in the tables, the equalities $d(n) = d(n+1) = d(n+2) = d(n+3) = 8$ hold for $n = 3655$, 4503, 5943, 6853, 7256, 8393, 9367.

As found by J. Mycielski, for $n = 40311$ we have

$$d(n) = d(n+1) = d(n+2) = d(n+3) = d(n+4).$$

The proof follows immediately from the factorizations into primes of the numbers $40311 = 3^3 \cdot 1493$, $40312 = 2^3 \cdot 5039$, $40313 = 7 \cdot 13 \cdot 443$, $40314 = 2 \cdot 3 \cdot 6719$, $40315 = 5 \cdot 11 \cdot 733$. A similar situation occurs for $n = 99655$.

A question has been asked for how many consecutive integers $d(n)$ can take the same value (cf. Erdös and Mirsky [1]). We have $d(2) = d(3)$, $d(14) = d(15)$, $d(33) = d(34) = d(35) = 4$, $d(242) = d(243) = d(244) = d(245) = 6$. D.R. Heath-Brown [1] has proved the existence of infinitely many n such that $d(n) = d(n+1)$.

We do not know whether there exists an infinite increasing sequence of natural numbers n_k ($k = 1, 2, \dots$) such that $\lim\limits_{k\to\infty} d(n_k+1)/d(n_k) = 2$. Neither do we know whether the numbers $d(n+1)/d(n)$ are dense in the set of the positive real numbers. However, P. Erdös has proved that they are dense in a non-trivial interval. (Cf. Erdös [14], footnote (¹).)

For $n \leqslant 10000$ we have $d(n) \leqslant 64$ and the maximum value $d(n) = 64$ is taken only for the numbers $n = 7560$ and 9240.

A. Schinzel [2] has proved that for all natural numbers h and m there exists a natural number $n > h$ such that

$$d(n)/d(n \pm i) > m \qquad \text{for} \qquad i = 1, 2, \dots, h.$$

2. Sums $d(1)+d(2)+\dots+d(n)$

For real numbers $x \geqslant 1$ we denote by $T(x)$ the sum

$$T(x) = \sum_{k=1}^{[x]} d(k) = d(1)+d(2)+\dots+d([x]). \tag{6}$$

In order to find this sum we prove first that for a given natural number k the number $d(k)$ is the number of the solutions of the equation

$$mn = k \tag{7}$$

in natural numbers m and n.

In fact, if a natural number n is a divisor of a number k, then $m = k/n$ is a natural number and the pair m, n is a solution of equation (7) in natural numbers. Conversely, if a pair of natural numbers m, n satisfies equation (7), then n is a divisor of the number k. Accordingly, to each natural divisor of the number k corresponds precisely one solution of equation (7) and *vice versa.* It follows that the number $d(k)$ is equal to the number of the solutions of equation (7) in natural numbers, and this is what was to be proved.

Consequently, in view of (6), $T(x)$ can be regarded as the number of solutions of the inequality $mn \leqslant [x]$ in natural numbers m, n, this being clearly equivalent to the inequality

$$mn \leqslant x. \tag{8}$$

All the solutions of the last inequality in natural numbers m, n we divide into classes simply by saying that a solution m, n belongs to the nth class. If k_n denotes the number of the solutions belonging to the nth class, then, clearly,

$$T(x) = k_1 + k_2 + k_3 + \ldots \tag{9}$$

We now calculate the number of the solutions of the nth class. For a given n the number m can take only the natural values satisfying inequality (8), i.e. the inequality

$$m \leqslant \frac{x}{n}.$$

This means that m can be any of the numbers $1, 2, \ldots, \left[\frac{x}{n}\right]$, which are $\left[\frac{x}{n}\right]$ in number. Therefore $k_n = \left[\frac{x}{n}\right]$, which, by (9) gives

$$T(x) = \left[\frac{x}{1}\right] + \left[\frac{x}{2}\right] + \left[\frac{x}{3}\right] + \ldots \tag{10}$$

The right-hand side of this equality is not an infinite series, in fact: only the first $[x]$ terms of it are different from zero. Thus formula (10) can be rewritten in the form

$$T(x) = \sum_{k=1}^{[x]} \left[\frac{x}{k}\right]. \tag{11}$$

The calculation of the number $T(x)$ from (11), though much more convenient than by finding the consecutive values of the function $d(k)$, is somewhat tedious for larger values of x. For instance, in order to find $T(100)$ by the use of (11) one has to add a hundred numbers. For this reason it seems worth-while to find a more convenient formula for $T(x)$.

In order to do this we divide the class of all the solutions of inequality (8) in natural numbers into two classes including in the first class the solutions for which $n \leqslant \sqrt{x}$ and in the second the remaining solutions, i.e. those for which $n > \sqrt{x}$. We calculate the number of the solutions in each of these two classes.

If n takes natural values $\leqslant \sqrt{x}$ and if m, n is a solution of inequality (8) in natural numbers, i.e. if m is a natural number such that $m \leqslant x/n$, then m, n belongs to the first class. Then for every natural number $n \leqslant \sqrt{x}$ the number of the solutions in the first class is $\left[\dfrac{x}{n}\right]$. Since n takes the values $1, 2, \ldots, [\sqrt{x}]$, the number of the solutions in the first class is

$$\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right].$$

We now calculate the number of the solutions belonging to the second class. That is we find how many of the pairs of natural numbers m, n satisfy the inequalities

$$mn \leqslant x \quad \text{and} \quad n > \sqrt{x},$$

i.e. the inequalities

$$\sqrt{x} < n \leqslant \frac{x}{m}. \tag{12}$$

If we had $m > \sqrt{x}$, then $x/m < \sqrt{x}$ and inequalities (12) would not be satisfied for any n. Accordingly, let m denote a fixed natural number $\leqslant \sqrt{x}$. In order to find the number of possible values of n for which inequalities (12) are satistfied, it is sufficient to subtract from the number of all the natural numbers $n \leqslant \dfrac{x}{m}$ $\left(\text{i.e. from the number } \left[\dfrac{x}{m}\right]\right)$ the number of the natural numbers n which do not satisfy the inequality $\sqrt{x} < n$, i.e. the number of the n's which satisfy the inequality $n \leqslant \sqrt{x}$ (clearly, they are $[\sqrt{x}]$ in number). Hence $\left[\dfrac{x}{m}\right] - [\sqrt{x}]$ is the number of all the pairs m, n which for $m \leqslant \sqrt{x}$ satisfy inequalities (12). But since m can take only the values 1, 2, ..., $[\sqrt{x}]$, the number of the pairs of natural numbers m, n satisfying inequalities (12), i.e. the number of the solutions belonging to the second class, is

$$\sum_{m=1}^{[\sqrt{x}]}\left(\left[\frac{x}{m}\right]-[\sqrt{x}]\right)=\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]-\sum_{m=1}^{[\sqrt{x}]}[\sqrt{x}].$$

The second of the sums on the right-hand side of the last equality is equal to the number $[\sqrt{x}]^2$ because it is the sum of $[\sqrt{x}]$ summands, each being equal to $[\sqrt{x}]$. Consequently, the number of the solutions in the second class is equal to

$$\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]-[\sqrt{x}]^2.$$

Thus, combining this with the number of the solutions belonging to the first class previously obtained, we get

$$\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]+\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]-[\sqrt{x}]^2$$

as the number of all the solutions of inequalities (8) in natural numbers m, n, i.e. the value of the function $T(x)$. We have $\sum_{m=1}^{[\sqrt{x}]}\left[\frac{x}{m}\right]=\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]$ because both the sums are abbreviated forms of the sum $\left[\frac{x}{1}\right]+\left[\frac{x}{2}\right]+\ldots+\left[\frac{x}{[\sqrt{x}]}\right]$; therefore we may write

$$T(x)=2\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]-[\sqrt{x}]^2. \tag{13}$$

This formula has been found by Lejeune Dirichlet. Applying it we calculate $T(100)$ as follows:

$$T(100)=2\sum_{n=1}^{10}\left[\frac{100}{n}\right]-10^2=2(100+50+33+25+20+$$
$$+16+14+12+11+10)-100=2\cdot 291-100=482.$$

Similarly, by an easy calculation, we find

$$T(200)=1098,\qquad T(500)=3190,\qquad T(1000)=7069.$$

Slightly longer calculations lead us to the values

$$T(5000)=43376,\qquad T(10000)=93668.$$

From formula (11) an approximate formula for the average value of the function $d(n)$ is easily obtainable. If on the right-hand side of formula (11) we replace $\left[\frac{x}{k}\right]$ simply by $\frac{x}{k}$, then the error in each of the summands is less than 1, and consequently in the whole sum it is less than the number of the summands, i.e. less than $[x] \leqslant x$. Therefore, as an approximate value of $T(x)$ we have $\sum_{n=1}^{[x]} \frac{x}{n}$, the error of the approximation being less than x. For natural values of $x = k$ we then have

$$\frac{d(1)+d(2)+\ldots+d(k)}{k} \approx \frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{k}, \tag{14}$$

the error of the approximation being less than 1. Since the right-hand side of (14) increases to infinity with k, the ratio of the left-hand side to the right-hand side of (14) tends to 1 when k tends to infinity.

As is known from Analysis, for the approximate value of the sum $\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{k}$ we may take the number $\log k$, the error being less than 1 for $k > 1$. Consequently, $\log k$ is an approximate value of the left-hand side of (14).

As one proves in Analysis, the difference $\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{k}-\log k$ tends to a finite limit called *Euler's constant* $C = 0.57721566\ldots$ (we do not know whether it is an irrational number). On the basis of this and formula (13) the expression $x\log x+(2C-1)x$ has been found, which approximates $T(x)$ with an error less than a finite multiple of $\sqrt{x}$. G. Voronoï proved that the error is not greater than a finite multiple of $\sqrt[3]{x}\,\log x$. Later other authors found a more precise evalution of this error (cf. Kolesnik [1]).

3. Numbers $d(n)$ as coefficients of expansions

The function $d(n)$ appears in Analysis as the coefficient of expansion in infinite series. For instance, consider the series (convergent for $|x| < 1$)

$$\sum_{k=1}^{\infty} \frac{x^k}{1-x^k} = \frac{x}{1-x}+\frac{x^2}{1-x^2}+\frac{x^3}{1-x^3}+\ldots$$

known under the name of *Lambert's series*. Expanding each if its terms into the geometrical progression

$$\frac{x^k}{1-x^k} = x^k + x^{2k} + x^{3k} + \dots$$

we obtain the double sum $\sum_{k=1}^{\infty} \sum_{l=1}^{\infty} x^{kl}$, in which for every natural number n the power x^n appears as many times as there are solutions of the equation $kl = n$ in natural numbers k and l, i.e. $d(n)$ times. Hence (for $|x| < 1$) we have

$$\sum_{k=1}^{\infty} \frac{x^k}{1-x^k} = \sum_{n=1}^{\infty} d(n)\, x^n.$$

We see that the function $d(n)$ is the coefficient at x^n in the expansion of Lambert's series in a power series.

The function $d(n)$ is also the coefficient in the expansion of the square of the ξ function. For $s > 1$ we consider an infinite series

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

(one proves in Analysis that the series is convergent for $s > 1$). Now we apply the so-called *Dirichlet multiplication* to the product $\zeta(s)\zeta(s)$.

Dirichlet's multiplication is as follows: given two series $a_1 + a_2 + \dots$ and $b_1 + b_2 + \dots$, we multiply $(a_1 + a_2 + \dots)$ by $(b_1 + b_2 + \dots)$ and put together those products $a_k b_l$ for which the products of indices are equal, i.e. $(a_1 + a_2 + \dots)(b_1 + b_2 + \dots) = a_1 b_1 + (a_1 b_2 + a_2 b_1) + (a_1 b_3 + a_3 b_1) + (a_1 b_4 + a_2 b_2 + a_4 b_1) + (a_1 b_5 + a_5 b_1) + (a_1 b_6 + a_2 b_3 + a_3 b_2 + a_6 b_1) + (a_1 b_7 + a_7 b_1) + \dots$ As can easily be seen this multiplication applied to $\zeta(s)$ gives

$$(\zeta(s))^2 = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}. \tag{15}$$

4. Sum of divisors

The sum of the natural divisors of a natural number n is denoted by $\sigma(n)$. It follows from Theorem 1 that if (1) is the factorization into primes of the number n, then

$$\sigma(n) = \sum q_1^{\lambda_1} q_2^{\lambda_2} \dots q_k^{\lambda_k}, \tag{16}$$

where the summation extends over all the systems of k integers (4) satisfying inequalities (3). But, as one easily sees, each summand of (16) is obtained in the expansion of the product

$$(1+q_1+q_1^2+\ldots+q_1^{\alpha_1})(1+q_2+q_2^2+\ldots+q_2^{\alpha_2})\ldots(1+q_k+q_k^2+\ldots+q_k^{\alpha_k})$$

precisely once.

On the other hand, each of the terms of the expansion of this product is one of the summands of the sum of (16). Hence

THEOREM 3. *The sum $\sigma(n)$ of the natural divisors of a natural number n whose factorization into primes is $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ is equal to*

$$(17) \qquad \sigma(n) = \frac{q_1^{\alpha_1+1}-1}{q_1-1}\cdot\frac{q_2^{\alpha_2+1}-1}{q_2-1}\ldots\frac{q_k^{\alpha_k+1}-1}{q_k-1}.$$

In particular, $\sigma(100) = \frac{2^3-1}{2-1}\cdot\frac{5^3-1}{5-1} = 7\cdot 31 = 217$.

It follows immediately from Theorem 3 that for natural numbers a, b, with $(a,b)=1$ we have $\sigma(ab)=\sigma(a)\sigma(b)$. It is easy to see that, if $(a,b)>1$, then $\sigma(ab)<\sigma(a)\sigma(b)$. Using Theorem 3, we can easily calculate $\sigma(1)=1$, $\sigma(2)=3$, $\sigma(3)=4$, $\sigma(4)=7$, $\sigma(5)=6$, $\sigma(6)=12$, $\sigma(7)=8$, $\sigma(8)=15$, $\sigma(9)=13$, $\sigma(10)=18$.

For $n>1$ we have $\sigma(n)>n$. It follows that $\sigma(n)>5$ for $n>4$. As one sees from the table presented above, $\sigma(n)$ takes for $n\leqslant 4$ the values 1, 3, 4 and 7. Therefore there is no natural number n for which $\sigma(n)=5$.

THEOREM 4. *There exist infinitely many natural numbers which are not the values of the function $\sigma(x)$ for natural x.*

PROOF. Let n be a natural number >9 and let k be a natural number such that

$$(18) \qquad \frac{n}{3}-1<k\leqslant\frac{n}{2}.$$

The number of the k's for which (18) holds is clearly greater than $n/2 - n/3 = n/6$. In virtue of (18) we have

$$(19) \qquad 2k\leqslant n \quad \text{and} \quad 3k+3>n,$$

and, since $n>9$, we have $3k>6$, which in consequence gives $k\geqslant 3$. Hence one sees that the number $2k$ has at least four different divisors: 1, 2, k, $2k$. Therefore $\sigma(2k)\geqslant 1+2+k+2k$, which, by (19), gives $\sigma(2k)>n$. Since the number of different natural numbers k for which (18) and (19) and consequently the inequality $\sigma(2k) > n$ hold is greater than $n/6$, then among the numbers $\sigma(1), \sigma(2), \ldots, \sigma(n)$ there are more than $n/6$ numbers greater than n. Hence in the sequence $1, 2, \ldots, n$ there are more than $n/6$ natural numbers which cannot be the values of the function $\sigma(x)$ for $x \leqslant n$. These numbers cannot be the values of the function $\sigma(x)$ for $x > n$ either, because the numbers are $\leqslant n$ and $\sigma(x) \geqslant 1+x > n$ for $x > n$. Therefore for every natural number $n > 9$ there are more than $n/6$ natural numbers in the sequence $1, 2, \ldots, n$ which cannot be the values of the function $\sigma(x)$ for natural values of x. This proves Theorem 4. □

Thus, there exist infinitely many natural numbers m for which the equation $\sigma(x) = m$ is insolvable in natural numbers x. It can be proved that all numbers $m = 3^k$ $(k > 1)$ have this property (cf. Sierpiński [27]). There are 59 such numbers $m \leqslant 100$. These are 2, 5, 9, 10, 11, 17, 19, 21, 22, 23, 25, 26, 27, 29, 33, 34, 35, 37, 41, 43, 45, 46, 47, 49, 50, 51, 52, 53, 55, 58, 59, 61, 64, 65, 66, 67, 69, 70, 71, 73, 75, 76, 77, 79, 81, 82, 83, 85, 86, 87, 88, 89, 92, 94, 95, 97, 99, 100. Among the remaining natural numbers $m \leqslant 100$ there are 25 for which the equation $\sigma(x) = m$ has precisely one solution in natural numbers. These are $m = 1, 3, 4, 6, 7, 8, 13, 14, 15, 20, 28, 30, 36, 38, 39, 40, 44, 57, 62, 63, 68, 74, 78, 91, 93$. This suggests the question whether there exist infinitely many natural numbers m for which the equation $\sigma(x) = m$ has precisely one solution. The answer in the affirmative follows from the more general theorem given below, which, according to P. Erdös [14], p. 12, states that if for any given k there exists a number m such that the equation $\sigma(x) = m$ has precisely k solutions, then there exist infinitely many such numbers m. It is much easier to prove, however, that there are infinitely many natural numbers m for which the equation $\sigma(x) = m$ has more than one solution. To this class belong, for instance, the numbers $m = 3(5^k - 1)$, where $k = 1, 2, \ldots$ The reason is that, in virtue of $\sigma(6) = \sigma(11) = 12$ and $(6,5^{k-1}) = (11,5^{k-1}) = 1$, we have $\sigma(6 \cdot 5^{k-1}) = \sigma(11 \cdot 5^{k-1}) = 3(5^k - 1)$.

It is easy to prove that there exist infinitely many natural numbers m for which the equation $\sigma(x) = m$ has more than two solutions. This property attaches, for instance, to the numbers $2(13^k - 1)$, where $k = 1, 2, \ldots$ In fact, we have $\sigma(14 \cdot 13^{k-1}) = \sigma(15 \cdot 13^{k-1}) = \sigma(23 \cdot 13^{k-1}) = 2(13^k - 1)$.

It is not known whether for every natural number k there exists a natural number m_k for which the equation $\sigma(x) = m_k$ has precisely k solutions in natural numbers x. This follows from the conjecture H (cf.

Schinzel [13]). It can be proved that if m_k denotes the least of the numbers for which $\sigma(x) = m_k$ has precisely k solutions, then $m_1 = 1, m_2 = 12, m_3 = 24, m_4 = 96, m_5 = 72, m_6 = 168, m_7 = 240, m_8 = 432, m_9 = 360, m_{10} = 504$, $m_{11} = 576$, $m_{12} = 1512$, $m_{13} = 1080$, $m_{14} = 1008$, $m_{15} = 720$, $m_{16} = 2304$, $m_{17} = 3600$, $m_{18} = 5376$, $m_{19} = 2160$, $m_{20} = 1440$.

The equation $\sigma(x) = m$ has precisely three solutions in natural numbers for the following six natural numbers $m \leqslant 100$, namely 24, 42, 48, 60, 84, 90.

The equation $\sigma(x) = m$ has precisely four solutions only for one natural number $m \leqslant 100$, namely for $m = 96$. It has precisely five solutions also for one natural number $m \leqslant 100$, namely for 72.

There is no natural number $m \leqslant 100$ for which the equation $\sigma(x) = m$ has more than five solutions in natural numbers; however, H. J. Kanold [2] has proved that for every natural number k there exists a natural number m such that the equation $\sigma(x) = m$ has $\geqslant k$ solutions in natural numbers x. The equation $\sigma(n) = \sigma(n+1)$ has only 9 solutions for $n < 10000$. These are $n = 14, 206, 957, 1334, 1364, 1634, 2685, 2974, 4364$ (cf. Mąkowski [4]). There are 113 solutions with $n \leqslant 10^7$ (Hunsucker, Nebb and Stearns [1], see also Guy and Shanks [1]). We do not know wherther there exist infinitely many natural numbers n for which $\sigma(n) = \sigma(n+1)$.

A. Mąkowski has asked whether for every integer k there exists a natural number n such that $\sigma(n+1) - \sigma(n) = k$ and, more generally, whether for every natural number m and every integer k there exists a natural number n such that $\sigma(n+m) - \sigma(n) = k$. Numerical results concerning $m \leqslant 5$ have been obtained by Mientka and Vogt [1].

If n and $n+2$ are twin prime numbers then $\sigma(n+2) = \sigma(n) + 2$. This equation, however, is also satisfied by the number $n = 434$, though the numbers 434 and 436 are not prime. A similar situation occurs for $n = 8575$ and $n = 8825$.

According to a conjecture of Catalan as corrected by Dickson [3] if $f(n) = \sigma(n) - n$, then for natural numbers $n > 1$ the infinite sequence of consecutive iterations of the function f

$$n,\ f(n),\ ff(n),\ fff(n), \ldots$$

either is periodic or terminates at the number 1. This is true for all $n \leqslant 275$ (cf. Devitt [1]). According to L. Alaoglu and P. Erdös [2] not only is the proof of this conjecture unknown, but also it is difficult to verify the conjecture for particular natural value of n. This is indeed the case for $n = 276$.

It is easy to see that for $n = 12496 = 2^4 \cdot 11 \cdot 71$ all the numbers $n, f(n)$, $ff(n), fff(n), ffff(n)$ are different and that $fffff(n) = n$, so the sequence is periodic. For $n = 12$, however, we have $f(12) = 16, f(16) = 15, f(15) = 9$, $f(9) = 4$, $f(4) = 3$, $f(3) = 1$, which shows that the sequence terminates at the number 1, which, of course, is also the case for a prime n, since then $f(n) = 1$. For $n = 100$ we have $f(100) = 117, f(117) = 65$, $f(65) = 19$, $f(19) = 1$. For $n = 6$, however, we have $f(n) = n$ and the sequence is trivially periodic, the period consisting of one term. For $n = 95$ we have $f(95) = 25$, $f(25) = 6$, $f(6) = 6$ and we see that the sequence is periodic from the fourth term onwards the period consisting of one term only. For $n = 220$ we have $f(220) = 284, f(284) = 220 = n$, and so the sequence is periodic from the very beginning onwards, the period consisting of two terms. In an unpublished typescript P. Poulet [3] has announced that for $n = 936$ the sequence 936, 1794, 2238, 2250,..., 74, 40, 50, 43, 1 is obtained, consisting of 189 terms, the greatest of them being 33 289 162 091 526.

This suggests the question whether there exist arbitrarily long sequences $n, f(n), ff(n), \ldots$ which terminate at 1 and whether there exist infinitely many natural numbers n for which the above sequence is periodic. The answer to this question is positive provided the conjecture that every even number greater than 6 is the sum of two different prime numbers is true.

In fact, suppose that this conjecture is true and let $2k-1$ denote an arbitrary odd number > 7. Then $2k-2 > 6$ and, according to the conjecture, there exist two different prime numbers p and q, both odd of course, such that $2k-2 = p+q$. Hence $f(pq) = \sigma(pq)-pq = 1+p+q = 2k-1$. Since p, q are two different odd primes, we have, say, $p > q$, and so $p \geqslant q+2$ and $q \geqslant 3$. Hence $pq \geqslant 3p = 2p+p \geqslant 2p+q+2 > p+q+1 = 2k-1$. Consequently $pq > 2k-1$. Therefore for every odd number $n > 7$ there exists an odd number $m > n$ such that $f(m) = n$. Let $m = g(n)$. Then the infinite increasing sequence $g(n), gg(n), \ldots$ is obtained. If for a natural number k we put $n = g^k(11)$ we get the sequence $n = g^k(11), f(n) = g^{k-1}(11), \ldots, f^k(n) = 11, f(11) = 1$, We have thus formed a decreasing sequence $n, f(n), ff(n), \ldots$ of $k+2$ terms, the last term being equal to 1.

If for a natural number k we put $n = g^k(25)$, we obtain the periodic sequence $n = g^k(25)$, $f(n) = g^{k-1}(25), \ldots, f^k(n) = 25$, $f(25) = 6$, $f(6) = 6, 6, \ldots$ with $k+1$ decreasing terms preceding the period.

There is another question which one may ask in this connection. This is whether there exist infinitely many different natural numbers for which the sequence $n, f(n), ff(n), \ldots$ is periodic and has no terms preceding the period. So far only periods of length 1, 2, 4, 5 and 28 have been discovered (cf. H. Cohen [1]).

We have just proved that the conjecture that every even natural number > 6 is a sum of two different prime numbers implies that every odd natural number > 7 is a term of the sequence $f(n)$ $(n = 1, 2, \ldots)$. Moreover, we have $f(3) = 1$, $f(4) = 3$, $f(8) = 7$. However, it is easy to prove that the number 5 does not occur in the sequence $f(n)$ $(n = 1, 2, 3, \ldots)$. In fact, if for a natural number n the equality $f(n) = \sigma(n) - n = 5$ could hold, then 5 would of course be a composite number (because $\sigma(1) - 1 = 0$ and, for a prime n, $\sigma(n) - n = 1$). So $n = ab$, where $1 < a \leqslant b < n$. Then, since $1, b$ and n would be different divisors of the number n, we would have $\sigma(n) \geqslant 1 + b + n$, whence $5 = \sigma(n) - n \geqslant 1 + b > b$, and so $b < 5$. Therefore we would have $n = ab$ with $1 < a \leqslant b \leqslant 4$. But, as can easily be verified, this is impossible, since there are no natural numbers a, b having the above properties for which the equation $\sigma(n) = n + 5$ is satisfied.

Without the conjecture that every even natural number > 6 is a sum of two different prime numbers we are unable to prove that every odd number different from 5 is for a suitably chosen natural number n a term of the sequence $\sigma(n) - n$ $(n = 1, 2, \ldots)$. P. Erdős [17] has proved that there exist infinitely many natural numbers which do not belong to this sequence.

It can be proved that the relation $m \mid \sigma(mn - 1)$ holds for all natural numbers n if and only if $m = 3, 4, 6, 8, 12$ or 24 (cf. Gupta [1]).

We do not know whether there exist infinitely many natural numbers n for which $\sigma(n)$ is the square of a natural number. The positive answer to this question can easily be derived from Conjecture H (Chapter III, § 8). In fact, let $f(x) = 2x^2 - 1$, the polynomial $f(x)$ is irreducible and, since $f(0) = -1$, it satisfies Condition C formulated in Chapter III. Therefore, according to Conjecture H, there exist infinitely many natural numbers x for which $p = 2x^2 - 1$ is a prime number > 7. For those x's we have $\sigma(7p) = 8(p+1) = (4x)^2$. This proves that $\sigma(7p)$ is the square of a natural number. We know some solutions of the equation $\sigma(x^3) = y^2$ in natural numbers, e.g. $x = 7$, $y = 20$. We also know some of the solutions of the equation $\sigma(x^2) = y^3$ in natural numbers, e.g. $x = 2 \cdot 3 \cdot 11 \cdot 653$, $y = 7 \cdot 13 \cdot 19$.

EXERCISES. 1. Prove that the equality $\sigma(n) = n+1$ holds if and only if n is a prime.

PROOF. If p is a prime number, then it has precisely two divisors, namely p and 1. Therefore $\sigma(p) = p+1$. On the other hand, if n is a composite number, i.e. if $n = ab$, where a and b are natural numbers > 1, then $1 < a < ab = n$ and consequently n has at least three different natural divisors: $1, a$ and n. Hence $\sigma(n) \geqslant 1+a+n > n+1$. Finally, if $n = 1$, then $\sigma(n) = 1 < n+1$. ☐

2. Prove that for every natural number m there exist natural numbers x, y such that $x-y \geqslant m$ and $\sigma(x^2) = \sigma(y^2)$.

PROOF. Let n be an arbitrary natural number $> m$ such that $(n, 10) = 1$. For $x = 5n, y = 4n$ we have $x-y = n > m$ and $\sigma(x^2) = \sigma(y^2) = 31\sigma(n^2)$. ☐

3. Find all the natural numbers whose divisors added up give odd sums.

SOLUTION. Suppose that n is a natural number such that $\sigma(n)$ is odd. Let $n = 2^\alpha k$, where k is an odd number and α is a non-negative integer. We have $\sigma(n) = (2^{\alpha+1}-1)\sigma(k)$ and consequently $\sigma(k)$ must be an odd number. Since k is odd, each of its divisors must be odd and, since the sum of the divisors $\sigma(k)$ is odd, the number of the divisors $d(k)$ must also be odd.

Hence, as we have learned in § 1, k must be the square of a natural number, i.e. $k = m^2$. Thus we see that $n = 2^\alpha m^2$. If α is even, that is if $\alpha = 2\beta$, then $n = (2^\beta m)^2$. If α is odd, then $\alpha = 2\beta+1$ and so $n = 2(2^\beta m)^2$. Hence either $n = l^2$ or $n = 2l^2$, where l is a natural number.

On the other hand, if $n = l^2$ or $n = 2l^2$, where l is a natural number, then $n = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$ is the factorization of n into primes, $q_1, q_2, \dots, q_k$ being odd prime numbers. We then have $\sigma(n) = (2^{2\alpha+1}-1)\sigma(q_1^{2\alpha_1})\dots\sigma(q_k^{2\alpha_k})$ or $\sigma(n) = (2^{2\alpha+2}-1)\sigma(q_1^{2\alpha_1})\dots\sigma(q_k^{2\alpha_k})$. But since the number $\sigma(q_i^{2\alpha_i}) = 1+q_i+q_i^2+\dots+q_i^{2\alpha_i}$, as the sum of an odd number of summands, each of them odd, is odd, the number $\sigma(n)$ is odd. Therefore the answer is that $\sigma(n)$ is odd if and only if n is either a square or a square multiplied by 2.

4. Prove that if n is a composite number, then $\sigma(n) > n+\sqrt{n}$.

PROOF. Being composite, n has a divisor d such that $1 < d < n$. Hence $1 < n/d < n$. If $d \leqslant \sqrt{n}$, then $n/d \geqslant \sqrt{n}$. But since n/d is also a divisor of n (not necessarily different from d) and $1 < n/d < n$, we see that $\sigma(n) \geqslant n+\sqrt{n}+1$, whence $\sigma(n) > n+\sqrt{n}$, which was to be proved. ☐

REMARK. As an easy consequence of the fact just proved, we note that $\lim\limits_{n\to\infty}\big(\sigma(p_n+1)-\sigma(p_n)\big) = +\infty$ and that $\lim\limits_{n\to\infty}\big(\sigma(p_n)-\sigma(p_n-1)\big) = -\infty$.

3. Prove that for every natural number $k > 1$ the equation $\sigma(n) = n+k$ has a finite $\geqslant 0$ number of solutions.

PROOF. If $\sigma(n) = n+k$, where k is a natural number > 1, then n must be a composite number and, according to Exercise 4, $\sigma(n) > n+\sqrt{n}$, which proves that $n < k^2$.

In particular, the equation $\sigma(n) = n+2$ has no solutions and the equation $\sigma(n) = n+3$ has precisely one solution, namely $n = 4$. ☐

6. Prove that $\lim\limits_{n\to\infty}\dfrac{\sigma(n!)}{n!} = +\infty$.

PROOF. It is easy to prove that $\sigma(m)/m$ is the sum of the reciprocals of the natural divisors of m. Since the divisors of the number $n!$ comprise at least the natural numbers $\leqslant n$, we see that

$$\frac{\sigma(n!)}{n!} \geqslant \frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{n}.$$

But, since

$$\lim_{n\to\infty}\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{n}\right) = +\infty, \quad \text{we have} \quad \lim_{n\to\infty}\frac{\sigma(n!)}{n!} = \infty. \quad \square$$

7. L. Alaoglu nad P. Erdős [1] call a natural number n *superabundant* if $\sigma(n)/n > \sigma(k)/k$ whenever $k < n$. Prove that there are infinitely many such numbers.

PROOF. Let $u_n = \sigma(n)/n$ for $n = 1, 2, \ldots$ It follows from Exercise 6 that the infinite sequence $u_1, u_2, \ldots$ has no upper bound. Therefore, in order to prove the theorem it is sufficient to prove the following more general theorem:

Every infinite sequence with real numbers as terms and with no upper bound contains infinitely many terms, each being greater than any of the preceding ones.

In fact, suppose that a sequence $u_1, u_2, \ldots$ has no upper bound. Then we have $\lim_{n\to\infty}\max(u_1, u_2, \ldots, u_n) = +\infty$ and for each natural number m there exists a natural number $l > m$ such that

$$a_l = \max(u_1, u_2, \ldots, u_l) > \max(u_1, u_2, \ldots, u_m).$$

In the sequence $u_1, u_2, \ldots, u_l$ there exist of course terms which are equal to a_l. Let u_n denote the first of them. We then have $n > m$, $n \leqslant l$ and $u_n > u_k$ for $k < n$. Thus we have shown that for every natural number $> m$ there exists a natural number $n > m$ such that $u_n > u_k$ whenever $k < n$. The theorem is thus proved. $\square$

8. A. K. Srinivasan [1] calls a natural number n a *practical number* if every natural number $\leqslant n$ is a sum of different divisors of the number n. Prove that for natural numbers $n > 1$ the number $2^{n-1}(2^n-1)$ is practical.

PROOF. If k is a natural number $\leqslant 2^n-1$, then, as we know, k is a sum of different numbers of the sequence $1, 2, 2^2, \ldots, 2^{n-1}$. On the other hand, if $2^n-1 < k \leqslant 2^{n-1}(2^n-1)$, then $k = (2^n-1)t+r$, where t is a natural number $\leqslant 2^{n-1}$ and $0 \leqslant r < 2^n-1$, so t and r are sums of different numbers of the sequence $1, 2, 2^2, \ldots, 2^{n-1}$. The proof follows at once. $\square$

For a necessary and sufficient condition for a natural number n to be a practical number, cf. Sierpiński [16]. See also Stewart [2], Margenstern [1].

10 is not a practical number, 100 and 1000 are.

9. Find a natural number m for which the equation $\sigma(x) = m$ has more than a thousand solutions.

SOLUTION. We use the following method, due to S. Mazur. Suppose that we have found s triples of prime numbers p_i, q_i, r_i $(i = 1, 2, \ldots, s)$, all of those $3s$ primes being different and, moreover,

$$(p_i+1)(q_i+1) = r_i+1, \quad i = 1, 2, \ldots, s. \tag{20}$$

Let

$$a_i^{(0)} = p_i q_i, \quad a_i^{(1)} = r_i, \quad i = 1, 2, \ldots, s. \tag{21}$$

For every sequence $\alpha_1, \alpha_2, \ldots, \alpha_s$ consisting of s numbers equal to 0 or 1 we put

$$(22) \qquad n_{\alpha_1,\alpha_2,\ldots,\alpha_s} = a_1^{(\alpha_1)} a_2^{(\alpha_2)} \ldots a_s^{(\alpha_s)}.$$

Since the numbers p_i, q_i, r_i, $i = 1, 2, \ldots, s$ are different primes, conditions (21) and (22) give

$$(23) \qquad \sigma(n_{\alpha_1,\alpha_2,\ldots,\alpha_s}) = \sigma(a_1^{(\alpha_1)})\,\sigma(a_2^{(\alpha_2)}) \ldots \sigma(a_s^{(\alpha_s)}).$$

In virtue of (21) we have

$$\sigma(a_i^{(0)}) = (p_i+1)(q_i+1), \qquad \sigma(a_i^{(1)}) = r_i+1, \qquad i = 1, 2, \ldots, s,$$

and consequently, by (20), $\sigma(a_i^{(0)}) = \sigma(a_i^{(1)}) = \sigma(r_i)$, for $i = 1, 2, \ldots, s$, and so $\sigma(a_i^{(\alpha_i)}) = \sigma(r_i)$, $i = 1, 2, \ldots, s$. Thus we see that formula (23) implies the equality

$$\sigma(n_{\alpha_1,\alpha_2,\ldots,\alpha_s}) = \sigma(r_1)\,\sigma(r_2) \ldots \sigma(r_s) = \sigma(r_1 r_2 \ldots r_s)$$

for each of 2^s sequences $\alpha_1, \alpha_2, \ldots, \alpha_s$.

The numbers $n_{\alpha_1,\alpha_2,\ldots,\alpha_s}$, which are 2^s in number, are all different because, in view of (22) and (21), their factorizations into prime numbers are different. Thus we have obtained 2^s different natural numbers, each having the same sum of divisors.

Thus, in order to find, say, 1024 natural numbers the sums of the divisors of which are equal, it is sufficient to find 10 triples of prime numbers p_i, q_i, r_i $(i = 1, 2, \ldots, 10)$ such that all thirty are different and equalities (20) hold for them. It is easy to check that the following triples satisfy these conditions.

2, 3, 11; 5, 7, 47; 13, 17, 251; 19, 23, 479; 29, 41, 1259; 31, 83, 2687;
43, 71, 3167; 59, 61, 3719; 53, 101, 5507; 83, 97, 8231.

It follows that for

$$m = 12 \cdot 48 \cdot 252 \cdot 480 \cdot 1260 \cdot 2688 \cdot 3168 \cdot 3720 \cdot 5508 \cdot 8232$$

the equation $\sigma(x) = m$ has at least 1024 solutions in natural numbers x.

5. Perfect numbers

There exist infinitely many natural numbers n such that the sum of the divisors of n excluding n is less than n. Such are, for instance, all the prime numbers and their natural powers. There exist also infinitely many natural numbers n such that the sum of the divisors of n excluding n is greater than n. For instance such are the numbers of the form $n = 2^k \cdot 3$, where $k = 2, 3, \ldots$ However, we do not know whether there exist infinitely many natural numbers n such that the sum of the divisors of n excluding n is equal to n itself. These are called *prefect numbers*.

There are 30 known perfect numbers. All of them are even and we do not know whether there exist any odd perfect numbers. It has benn proved that if such a perfect number exists must be greater than 10^{50} (Buxton and Elmore [1] claim even 10^{200}) and must have at least eight different prime factors (Hagis [1], [2]). The greatest of the known perfect numbers is the number $2^{216090}(2^{216091}-1)$ which has 130100 digits. The least perfect number is the number $6 = 1+2+3$ and the next is $28 = 1+2+4+7+14$. The sum of the divisors of number n, each of them less than n, is of course the number $\sigma(n)-n$. Accordingly, a natural number is a perfect number if $\sigma(n)-n = n$, i.e. if it satisfies the equation

$$\sigma(n) = 2n. \tag{24}$$

THEOREM 5. *In order that an even number n be perfect it is necessary and sufficient that it should be of the form* $2^{s-1}(2^s-1)$, *where s is a natural number and* 2^s-1 *is a prime.*

PROOF. Let n be an even perfect number. Then $n = 2^{s-1}l$, where $s > 1$ and l is an odd number. Hence $\sigma(n) = (2^s-1)\sigma(l)$ and in virtue of (24), $(2^s-1)\sigma(l) = 2^s l$. Since $(2^s-1, 2^s) = 1$, we see that $\sigma(l) = 2^s q$, where q is a natural number. Hence $(2^s-1)q = l$, which, in view of $\sigma(l) = 2^s q$, implies $\sigma(l) = l+q$. But, in virtue of $(2^s-1)q = l$, we have $q \mid l$ and $q < l$ (because $s > 1$). Consequently, the number l has at least two different natural divisors, q and l, and the formula $\sigma(l) = l+q$ proves that it has no other divisors. Consequently, we see that $q = 1$ and that l is a prime number. But $l = (2^s-1)q = 2^s-1$. Therefore $n = 2^{s-1}l = 2^{s-1}(2^s-1)$, and so 2^s-1 is a prime number. Thus we have proved the necessity of the condition.

In order to prove the sufficiency we suppose that 2^s-1 is a prime number (of course an odd one). Further, let $n = 2^{s-1}(2^s-1)$. We have $\sigma(n) = (2^s-1)\sigma(2^s-1) = (2^s-1)2^s$ since 2^s-1 is a prime number. So $\sigma(n) = 2n$, which proves that n is a perfect number; this proves the sufficiency of the condition and, at the same time, completes the proof of the theorem. □

It is easy to prove that, if 2^s-1 is a prime number, then s must be also a prime. In fact, if $s = ab$, where a and b are natural numbers > 1, then

$$2^s-1 = (2^a-1)(1+2^a+2^{2a}+\ldots+2^{(b-1)a}),$$

which shows that, since $a > 1$, i.e. $a \geqslant 2$, and thus $2^a-1 \geqslant 2^2-1 \geqslant 3$, the number 2^s-1 is composite.

Thus Theorem 5 implies the following

COROLLARY. *All the even perfect numbers are given by the formula* $2^{p-1}(2^p-1)$, *where p and* 2^p-1 *are prime numbers.*

Perfect numbers were investigated by Euclid, eho discovered the following method of finding them:

"We calculate the consecutive sums of the series $1+2+4+8+16+32+\ldots$ If a sum turns out to be a prime, we multiply it by its last summand and obtain a perfect number".

Using Theorem 5 we see that the method of Euclid indeed gives all even perfect numbers.

Now we are going to find some of the even perfect numbers. In order to do this, we let p be consecutive prime numbers starting from number 2 and we look whether the number 2^p-1 is prime or not. We see that for $p=2, 3, 5, 7$ the numbers $2^p-1=3, 7, 31, 127$ are prime. This gives the first four perfect numbers, which were actually known in antiquity. They are $2(2^2-1)=6$, $2^2(2^3-1)=28$, $2^4(2^5-1)=496$, $2^8(2^7-1)=8128$. For $p=11$ the number $2^{11}-1=23\cdot 89$ is composite, and so we do not obtain a perfect number.

It follows from Theorem 5 that the task of finding even perfect numbers is the same as that of finding *Mersenne numbers* defined as being prime numbers of the form 2^s-1. We shall return to the latter problem in Chapter X.

We denote by $V(x)$, x being a real number, the number of perfect numbers $\leqslant x$. B. Hornfeck and E. Wirsing [1] have proved that $\lim\limits_{x\to\infty}\dfrac{\log V(x)}{\log x}=0$ and E. Wirsing [1] has proved that there exists a natural number A such that $V(x)<Ae^{A(\log x)/\log\log x}$.

We do not know whether there exist infinitely many natural numbers n such that $n\mid\sigma(n)$, or whether there exist odd natural numbers with this property. It has been proved that there are no such numbers n with $n<10^{50}$ (Beck and Najar [1]).

Natural numbers n such that $\sigma(n)=mn$, where m is a natural number >1, are called *P_m numbers* or *multiply perfect numbers*. These numbers were investigated by Mersenne, Fermat, Descartes, Legendre, and others.

Accordingly, P_2 numbers are perfect numbers. P. Poulet [1], (pp. 9–27) has found 334 P_m numbers with $m\leqslant 8$.

In 1953 B. Franqui and M. Garcia [1] obtained 63 new P_m numbers (cf. also Franqui and Garcia [2], A. L. Brown [1] and [2]). The numbers P_3 were investigated by R. Steuerwald [1].

P. Cattaneo [1] called a number *quasi-perfect* if it is equal to the sum of its own non-trivial natural divisors, i.e. the divisors different from 1 and the number itself. Accordingly, quasi-perfect numbers are those natural numbers n for which $\sigma(n) = 2n+1$. We do not know whether there are any such numbers. P. Hagis Jr. and G. L. Cohen [1] have proved that if they exist then they exceed 10^{35} and have at least seven distinct prime factors. However, it is easy to prove that there exist infinitely many natural numbers n such that $\sigma(n) = 2n-1$. For instance, such are all the numbers 2^k with $k = 0, 1, 2, \ldots$ A. Mąkowski [5] has investigated the solutions of the equation $\sigma(n) = 2n+2$ in natural numbers. He has noticed that, if 2^k-3 is a prime number, then $n = 2^{k-1}(2^k-3)$ is a solution of this equation. The numbers 2^k-3 are prime for the following values of $k < 24$: $k = 2, 3, 4, 5, 6, 9, 10, 12, 14, 20, 22$. The equation has also other solutions, e.g. $n = 650$. A more general equation $\sigma(n) = kn+a$ has been investigated by C. Pomerance [1] and A. Mąkowski [9].

EXERCISES. 1. Prove that there exist infinitely many odd natural numbers n such that $\sigma(n) > 2n$.

PROOF. Such are for instance the numbers $n = 945m$, where m is a natural number which is not divisible by 2, 3, 5, 7. Since $945 = 3^3 \cdot 5 \cdot 7$, $(m, 945) = 1$ and so $\sigma(n) = \sigma(945)\sigma(m) \geqslant \sigma(945)m = 1920m > 2n$. Since m is not divisible by 2, n is an odd number.

It can be proved that 945 is the least odd natural number for which $\sigma(n) > 2n$ holds. ☐

2. Find all the natural numbers n such that n is equal to the product of all the natural divisors of n excluding n.

SOLUTION. Let Q_n denote the product of all the natural divisors of number n. We are looking for natural numbers n such that $Q_n/n = n$, i.e. for numbers n for which $Q_n = n^2$. If $d_1, d_2, \ldots, d_s$ are all the natural divisors of number n (which are $s = d(n)$ in number), then the numbers $n/d_1, n/d_2, \ldots, n/d_s$ are also natural divisors of the number n. It follows that $Q_n = d_1 d_2 \ldots d_s = n^s/Q_n$, and so $Q_n = n^{s/2} = n^{d(n)/2}$. Since $Q_n = n^2$, we see that $n^2 = n^{d(n)/2}$, whence $d(n) = 4$, and as can easily be verified, the converse is also true: if $d(n) = 4$, then $Q_n = n^2$. Therefore, in order that a natural number be equal to the product of the natural divisors of n excluding n, it is necessary and sufficient that n have precisely four natural divisors. It follows from the formula for the number of divisors given by (5) that, provided (1) is the factorization of n into primes, the equality

$$(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1) = 4$$

holds. Since the exponents $\alpha_1, \alpha_2, \ldots, \alpha_k$ are natural numbers, the above formula is valid only in the case where $k \leqslant 2$, i.e. for $k = 1$ or $k = 2$. If $k = 1$, then $\alpha_1+1 = 4$, whence $\alpha_1 = 3$ and n turns out to be the cube of a prime number. If $k = 2$, then $\alpha_1 = \alpha_2 = 1$ and n turns out to be a product of two different primes. Thus we see that every natural number n which is the product of its own divisors less than n is either the cube of a prime numbers or the product of two different primes. The following are all the numbers of this kind that are less than 30: 6, 8, 10, 14, 15, 21, 22, 26, 27.

3. Prove the following theorem of Descartes (mentioned in a letter to Mersenne of 15th November 1638):

1 If n is a P_3 number and is not divisible by 3, then $3n$ is a P_4 number.

2 If a number n is divisible by 3 but not divisible either by 5 or by 9 and, moreover, if it is a P_3 number, then $45n$ is P_4.

3 If a number n is not divisible by 3 and if $3n$ is a P_{4k} number, then n is a P_{3k} number.

PROOF. 1 If n is a P_3 number, then $\sigma(n) = 3n$ and if n is not divisible by 3, then $\sigma(3n) = \sigma(3)\sigma(n) = 4\cdot 3n$ and consequently $3n$ is a P_4 number.

2 If n is a P_3 number and $n = 3k$, where k is divisible neither by 3 nor by 5, then $\sigma(45n) = \sigma(3^3\cdot 5k) = \sigma(3^3)\sigma(5)\sigma(k) = 40\cdot 6\cdot\sigma(k)$. But, in virtue of $n = 3k$ and k not being divisible by 3, we have $\sigma(n) = \sigma(3)\sigma(k) = 4\sigma(k)$. Consequently, $\sigma(45n) = 60\cdot 4\sigma(k) = 60\sigma(n)$. Hence, in view of n being a P_3 number $\sigma(n) = 3n$, we see that $\sigma(45n) = 180n = 4\cdot 45n$, which proves that $45n$ is a P_4 number.

3 If n is not divisible by 3 and if $3n$ is a P_{4k} number, then $\sigma(3n) = 4k\cdot 3n$, which implies that $\sigma(3n) = \sigma(3)\sigma(n) = 4\sigma(n)$, whence $\sigma(n) = 3kn$, which proves that n is a P_{3k} number. □

4. Prove that 120 and 672 are P_3 numbers, the number $2^5\cdot 3^3\cdot 5\cdot 7$ is a P_4 number, and $2^7\cdot 3^4\cdot 5\cdot 7\cdot 11^2\cdot 17\cdot 19$ is a P_5 number.

The proof follows at once if we look at the factorizations into primes of the numbers $120 = 2^3\cdot 3\cdot 5$ and $672 = 2^5\cdot 3\cdot 7$. It can be proved that 120 is the least P_3 number.

5. Prove that, if $\sigma(n) = 5n$, then n has more than 5 different prime factors.

PROOF. Suppose that (1) is the factorization of n into primes. Then, by (17), one has

$$\sigma(n) < \frac{q_1^{\alpha_1+1}q_2^{\alpha_2+1}\dots q_k^{\alpha_k+1}}{(q_1-1)(q_2-1)\dots(q_k-1)} = \frac{q_1}{q_1-1}\cdot\frac{q_2}{q_2-1}\cdot\dots\cdot\frac{q_k}{q_k-1}\cdot n.$$

If $k \leqslant 5$, then we would have

$$\sigma(n) \leqslant \frac{2}{1}\cdot\frac{3}{2}\cdot\frac{5}{4}\cdot\frac{7}{6}\cdot\frac{11}{10}n = \frac{77}{16}n < 5n$$

which contradicts the equality $\sigma(n) = 5n$. □

6. Prove the following theorem of Mersenne. If n is not divisible by 5 and it is a P_5 number, then $5n$ is a P_6 number.

The proof is straightforward.

6. Amicable numbers

Two natural numbers are called *amicable numbers* if each of them is equal to the sum of all the natural divisors of the other except the number itself. It is easy to see that in order that two natural numbers n, m be amicable it is necessary and sufficient that $\sigma(m) = \sigma(n) = m+n$.(¹)

The first pair of amicable numbers, 220 and 284, was found by

---

(¹) Editor's note. Most authors assume that $n \neq m$.

Pythagoras. The pair $2^4 \cdot 23 \cdot 47$ and $2^4 \cdot 1151$ was discovered by Fermat (¹), the pair $2^7 \cdot 191 \cdot 383$ and $2^7 \cdot 73727$ by Descartes. As many as 59 pairs of amicable numbers were found by Euler, among them the pair $2^3 \cdot 17 \cdot 79$ and $2^3 \cdot 23 \cdot 59$ and the pair $2^3 \cdot 19 \cdot 41$ and $2^5 \cdot 199$. A longer paper devoted to the amicable numbers has been written by E. J. Lee and J. S. Madachy [1]: they have presented a list of 1107 pairs of amicable numbers found in the last 25 centuries. The list is complete up to 10^8. More than 5000 new amicable pairs have been constructed by W. Borho, H. Hoffman and H. J. J. te Riele (see te Riele [1], [2]).

We know pairs of amicable numbers which are all odd, e.g. the pair $3^3 \cdot 5 \cdot 7 \cdot 11$, $3 \cdot 5 \cdot 7 \cdot 139$. But we do not know any pair with one of the numbers odd and the other even. Neither do we know whether there exist infinitely many pairs of amicable numbers.

The notion of a pair of amicable numbers has been generalized to the notion of a k-tuplet of amicable numbers. The notion is due to L. E. Dickson, who calls a k-tuplet of natural numbers $n_1, n_2, \ldots, n_k$ a *k-tuplet of amicable numbers* if

$$\sigma(n_1) = \sigma(n_2) = \ldots = \sigma(n_k) = n_1 + n_2 + \ldots + n_k$$

(Dickson [2], cf. also Mason [1]).

A. Mąkowski [4] has found the following triples of amicable numbers: $2^2 \cdot 3^2 \cdot 5 \cdot 11$, $2^5 \cdot 3^2 \cdot 7$, $2^2 \cdot 3^2 \cdot 71$ and $2^3 \cdot 3 \cdot 5 \cdot 13$, $2^2 \cdot 3 \cdot 5 \cdot 29$, $2^2 \cdot 3 \cdot 5 \cdot 29$ (in the second triple two of the numbers are equal). There exist triples for which all three numbers are equal, e.g. $n_1 = n_2 = n_3 = 120$.

A different definition of a k-tuplet of amicable numbers has been given by B. F. Yanney [1]. The definition is as follows: a k-tuplet of natural numbers $n_1, n_2, \ldots, n_k$ is called a *k-tuplet of amicable numbers* if

$$n_1 + n_2 + \ldots + n_k + \sigma(n_i) = \sigma(n_1) + \sigma(n_2) + \ldots + \sigma(n_k),$$
$$i = 1, 2, \ldots, k,$$

this being clearly equivalent to the condition

$$n_1 + n_2 + \ldots + n_k = (k-1)\,\sigma(n_i) \quad \text{for} \quad i = 1, 2, \ldots, k.$$

For $k = 2$ both definitions reduce to the ordinary definition of a pair of amicable numbers.

(¹) According to W. Borho [1] this been discovered already by Ibn Al-Banna (1256-1321).

For $k > 2$, however, the definitions no longer coincide and a k-tuplet, which is a k-tuplet of amicable numbers according to one definition is not a k-tuplet of amicable numbers according to the other. An example of a triple which is a triple of amicable numbers according to the definition of Yanney is the triple 308, 455, 581.

We have $308 = 2^2 \cdot 7 \cdot 11$, $455 = 5 \cdot 7 \cdot 13$, $581 = 7 \cdot 83$, so $\sigma(n_1) = \sigma(n_2) = \sigma(n_3) = 672$ and $n_1 + n_2 + n_3 = 1344 = 2 \cdot 672$.

It is not known whether there are pairs of relatively prime amicable numbers. H. J. Kanold [1] has proved that if in a pair m_1, m_2 of amicable numbers the numbers m_1, m_2 are relatively prime, then each of them must be greater than 10^{23} and the number $m_1 m_2$ must have more than 20 prime factors.

P. Erdös [13] has proved that, if $A(x)$ is the number of the pairs of amicable numbers $\leqslant x$, then $\lim\limits_{x \to \infty} A(x)/x = 0$.

C. Pomrance [2] has proved that, if $A(x)$ is the number of the pairs of amicable numbers $\leqslant x$ then for x large enough

$$A(x) < x \exp\left(-(\log x)^{1/3}\right).$$

7. The sum $\sigma(1) + \sigma(2) + \ldots + \sigma(n)$

In this section we are going to find the formula for the sum

$$S(x) = \sigma(1) + \sigma(2) + \ldots + \sigma([x]), \tag{25}$$

where x is a real number $\geqslant 1$.

Let n be a natural number. The number n is a term of the sum $\sigma(k)$ if and only if n is a divisor of the number k. Therefore, in order to calculate the number of the summands $\sigma(k)$ in the sum $S(x)$ in which n appears as a summand, it is sufficient to find the number of the k's $\leqslant x$ which are divisible by n. But those are the numbers k for which $k = nl \leqslant x$, where l is a natural number satisfying of course the inequality $l \leqslant x/n$. Clearly, the number of l's is $[x/n]$. Accordingly, a natural number n is a summand of the sum of $\sigma(k)$ for $[x/n]$ different natural numbers $k \leqslant x$. From this we infer that

$$S(x) = \sum_{n=1}^{[x]} n\left[\frac{x}{n}\right]. \tag{26}$$

There is another method of finding sum (25). In fact, the number $\sigma(k)$ can be thought of as the sum of natural numbers n satisfying the equation

$$mn = k,$$

where m is a natural number. Therefore sum (25) can be regarded as the sum of the numbers n for which there exist natural numbers m such that $mn \leqslant x$. Then for a fixed number m number n can be any of the numbers

$$1, 2, 3, \ldots, \left[\frac{x}{m}\right],$$

the sum of those being equal to

$$1+2+\ldots+\left[\frac{x}{m}\right]=\frac{1}{2}\left[\frac{x}{m}\right]^2+\frac{1}{2}\left[\frac{x}{m}\right].$$

Consequently, if we let m to take all the possible values for which the inequality $mn \leqslant x$ can be satisfied, the sum of all n's, i.e. the sum $S(x)$, is equal to

$$S(x)=\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]^2+\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]. \tag{27}$$

Comparing (26) and (27) we find the identity

$$\sum_{n=1}^{[x]} n\left[\frac{x}{n}\right]=\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]^2+\frac{1}{2}\sum_{m=1}^{[x]}\left[\frac{x}{m}\right]$$

which is of some interest in itself. Clearly, it can also be written in the form

$$\sum_{n=1}^{[x]}\left[\frac{x}{n}\right]^2=\sum_{n=1}^{[x]}(2n-1)\left[\frac{x}{n}\right].$$

Neither of the formulae (26), (27) is of any practical use for finding the numerical values of the sum $S(x)$ for a given number x. A formula more suitable for this purpose is to be found in a similar way as formula (13) was found and is as follows:

$$S(x)=\frac{1}{2}\left(\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right]^2+\sum_{n=1}^{[\sqrt{x}]}(2n+1)\left[\frac{x}{n}\right]-[\sqrt{x}]^3-[\sqrt{x}]^2\right). \tag{28}$$

For instance, with the use of this formula we can easily calculate $S(100) = 8249$.

Now, if in (28) we drop the symbol [ ] and replace the sum $\sum_{n=1}^{[\sqrt{x}]} 1/n^2$ by the sum of the infinite series $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$, each time calculating the error it involves, then we obtain the value $\pi^2 x^2/12$ as an approximation of the sum $S(x)$, the error being not greater than $Ax\sqrt{x}$, where A is a positive constant independent of x.

8. The numbers $\sigma(n)$ as coefficients of various expansions

The function $\sigma(n)$ (similarly to the function $d(n)$; cf. § 3) appears as the coefficient in various expansions in infinite series.

As is known from Analysis, the iterated series

$$\sum_{k=1}^{\infty} \sum_{l=1}^{\infty} kx^{kl} \tag{29}$$

is absolutely convergent for $|x| < 1$. Reducing it to an ordinary series, for a fixed value of n we put together the summands in which x^n appears. Then the coefficients of the nth groups of summands are the factors of the number $n = kl$. Consequently, the sum (29) turns into the sum $\sum_{n=1}^{\infty} \sigma(n) x^n$.

On the other hand, since $\sum_{l=1}^{\infty} kx^{kl} = kx^k/(1-x^k)$, we see that sum (29) is equal to the sum $\sum_{k=1} kx^k/(1-x^k)$. Thus we arrive at the formula

$$\sum_{k=1}^{\infty} \frac{kx^k}{1-x^k} = \sum_{n=1}^{\infty} \sigma(n) x^n, \qquad |x| < 1.$$

Since (29) is absolutely convergent for $|x| < 1$, we may interchange the elements of the series in such a way that, applying the identity $\sum_{k=1}^{\prime} kx^{kl} = x^l/(1-x^l)^2$, where $|x| < 1$, we obtain the formula

$$\sum_{l=1}^{\infty} \frac{x^l}{(1-x^l)^2} = \sum_{n=1}^{\infty} \sigma(n) x^n \qquad \text{for} \qquad |x| < 1.$$

In § 3 we have introduced Dirichlet's multiplication of two infinite series $a_1 + a_2 + \ldots$ and $b_1 + b_2 + \ldots$ We apply it here to the case where $a_k = 1/k^{s-1}$, $b_l = 1/l^s$, k and l being natural numbers and s being a real number > 2. We then have

$$a_k b_l = \frac{1}{k^{s-1}} \cdot \frac{1}{l^s} = \frac{k}{(kl)^s}.$$

Now, putting together the products $a_k b_l$ for which kl is equal to a given natural number n, we see that their numerators are equal to the natural divisors k of the number n; the sum of those being, clearly, $\sigma(n)/n^s$. Hence

$$\zeta(s-1)\zeta(s) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} \quad \text{for} \quad s > 2.$$

9. Sums of summands depending on the natural divisors of a natural number n

Let $f(n)$ be an arbitrary function defined for every natural number n. If $d_1, d_2, \ldots, d_s$ are all the divisors of a natural number n, then the sum

$$f(d_1)+f(d_2)+ \ldots +f(d_s)$$

is denoted simply by

$$\sum_{d|n} f(d)$$

and called the sum of the summands $f(d)$ with d ranging over the natural divisors of the number n. In particular, we have

$$\sum_{d|n} 1 = d(n), \qquad \sum_{d|n} d = \sigma(n) \qquad \text{but also} \qquad \sum_{d|n} \frac{n}{d} = \sigma(n).$$

For a given function $f(n)$ defined for natural numbers n we write

$$F(n) = \sum_{d|n} f(d).$$

Let us find the sum

$$\sum_{n=1}^{[x]} F(x) = \sum_{n=1}^{[x]} \sum_{d|n} f(d)$$

for the real values $x \geqslant 1$.

The sum on the right-hand side of the last formula comprises the summands $f(k)$, where k are natural numbers $\leqslant x$.

For a given natural number $k \leqslant x$ the summand $f(k)$ appears in the sum $\sum_{d|n} f(d)$ if and only if k is a divisor of number n. (Clearly, it appears at most once). The number of such natural numbers $n \leqslant x$ is of course $\left[\frac{x}{k}\right]$.

Consequently, the number of the summands $f(k)$ in the double sum is $\left[\frac{x}{k}\right]$, whence

$$\sum_{n=1}^{[x]} F(n) = \sum_{k=1}^{[x]} f(k)\left[\frac{x}{k}\right]. \tag{30}$$

In particular, if $f(n) = n^s$, where s is a fixed integer, then $F(n)$ is the sum of the sth powers of the natural divisors of the natural number n. This sum is sometimes denoted by $\sigma_s(n)$. Then formula (30) gives

$$\sum_{n=1}^{[x]} \sigma_s(n) = \sum_{k=1}^{[x]} k^s\left[\frac{x}{k}\right].$$

We have of course $\sigma_0(n) = d(n)$, $\sigma_1(n) = \sigma(n)$ for $n = 1, 2, \ldots$ and we see that formulae (11) and (26) are particular cases of the last formula.

10. The Möbius function

Under this name we mean the arithmetical function $\mu(n)$ defined by the conditions

1° $\mu(1) = 1$,

2° $\mu(n) = 0$ if the natural number n is divisible by the square of a natural number > 1,

3° $\mu(n) = (-1)^k$ if the natural number n is the product of k different prime factors.

Accordingly, $\mu(1) = 1$, $\mu(2) = \mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = \mu(9) = 0$, $\mu(10) = 1$.

Now we are going to show a certain property of the function $\mu(n)$. Let n be a natural number > 1 whose factorization into prime numbers is as in (1). Consider the product

$$(1-q_1^s)(1-q_2^s)\ldots(1-q_k^s), \tag{31}$$

where s is a given integer.

The expansion of product (31) consists of the number 1 and the numbers $\pm d^s$, where d is a divisor of number n, being a product of different prime factors; the sign $+$ or $-$ at each of the numbers appears according to whether the number is the product of an even or of an odd number of prime factors. In virtue of property 3° of the definition of the Möbius function, we see that the coefficient $\pm$ at d^s is equal to $\mu(d)$.

If, in addition, we note that $\mu(1)\cdot 1^s = 1$ and that, in order that the number d be equal to 1 or to the product of different prime numbers, it is necessary and sufficient that the number n have no divisor which is the square of a natural number > 1, then, by property 2°, we see that the product (31) is equal to the sum

$$\sum_{d|n} \mu(d)\, d^s.$$

That is

$$(1-q_1^s)(1-q_2^s)\dots(1-q_k^s) = \sum_{d|n} \mu(d)\cdot d^s,$$

whence for $s = 0$ we obtain

$$\sum_{d|n} \mu(d) = 0 \tag{32}$$

for every natural number $n > 1$. Clearly, for $n = 1$, we have $\sum_{d|1} \mu(d) = \mu(1) = 1$. We see that, if $F(n) = \sum_{d|n} \mu(d)$, then $F(1) = 1$ and $F(n) = 0$ for natural numbers $n > 1$. Consequently, formula (30) gives

$$\sum_{k=1}^{[x]} \mu(k)\left[\frac{x}{k}\right] = 1 \qquad \text{for} \qquad x \geqslant 1. \tag{33}$$

Since the inequalities $0 \leqslant t-[t] < 1$ hold for all real numbers t and since $|\mu(k)| \leqslant 1$ for natural numbers k, we see that $\left|\mu(k)\left[\frac{x}{k}\right] - \mu(k)\frac{x}{k}\right| < 1$ is valid whenever x is a real number $\geqslant 1$ and k is a natural number. From this we deduce that, if we drop the symbol [ ] in each of the summands of (33), then the error thus obtained is less than 1 and in the first summand is equal precisely to $x-[x]$. Thus, since there are $[x]-1$ summands in the sum excluding the first term, we have

$$\left|\sum_{k=1}^{[x]} \mu(k)\left[\frac{x}{k}\right] - x\sum_{k=1}^{[x]} \frac{\mu(k)}{k}\right| < x-[x]+[x]-1 = x-1,$$

whence, by (33), we obtain

$$\left|1 - x\sum_{k=1}^{[x]} \frac{\mu(k)}{k}\right| < x-1,$$

and this implies $|x \sum_{k=1}^{[x]} \mu(k)/k| \leqslant x$ and consequently $|\sum_{k=1}^{[x]} \mu(k)/k| \leqslant 1$.

This proves that the modulus of each of the partial sums of the infinite series

(34) $$\frac{\mu(1)}{1}+\frac{\mu(2)}{2}+\frac{\mu(3)}{3}+\dots$$

is $\leqslant 1$. As was proved by H. von Mangoldt in 1897, sum (34) is equal to 0. This had already been conjectured by Euler in 1748.

Now, we apply Dirichlet's multiplication to the series $\sum\limits_{k=1}^{\infty}\mu(k)/k^s$ and $\sum\limits_{l=1}^{\infty} 1/l^s$, where s is a natural number > 1. In virtue of $\mu(1) = 1$ and formula (32) we obtain

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k^s}\cdot\sum_{l=1}^{\infty}\frac{1}{l^s}=1,$$

i.e. the formula

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k^s}=\frac{1}{\zeta(s)},$$

s being a real number > 1. In particular, since, as is known from Analysis, $\zeta(2) = \pi^2/6$, the last equality implies

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}=\frac{6}{\pi^2}.$$

In this connection we observe, that it is easy to prove the equality

$$\sum_{k=1}^{\infty}\frac{\mu^2(k)}{k^s}=\frac{\zeta(s)}{\zeta(2s)},$$

where s is a real number > 1.

Reducing the iterated series $\sum\limits_{k=1}^{\infty}\sum\limits_{l=1}^{\infty}\mu(k)\,x^{kl}$ to an ordinary serries by the method we applied previously to the series (29), for $|x| < 1$ we obtain the formula

$$\sum_{n=1}^{\infty}\frac{\mu(n)\,x^n}{1-x^n}=x.$$

THEOREM 6. *For every arithmetical function $F(n)$ there exists only one arithmetical function $f(n)$ such that the equality*

(35) $$F(n)=\sum_{d\mid n} f(d)$$

holds for all natural numbers n.

PROOF. If, for $n = 1, 2, \ldots$, formula (35) is valid, then the following infinite sequence of equalities holds:

$$\begin{aligned} F(1) &= f(1), \\ F(2) &= f(1)+f(2), \\ F(3) &= f(1)+f(3), \\ F(4) &= f(1)+f(2)+f(4), \\ F(5) &= f(1)+f(5), \\ F(6) &= f(1)+f(2)+f(3)+f(6) \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{36}$$

The first equality gives $f(1) = F(1)$. So $f(2)$ can be calculated from the second equality. Then, since $f(1)$ and $f(2)$ have already been found, $f(3)$ can be calculated from the third equality and so on. The nth equality gives the value of $f(n)$, provided the values of $f(k)$ for $k < n$, have already been found from the previous equalities. Therefore we see that if there exists a function satisfying formula (35), then there is only one such function. On the other hand, it is easy to see that, calculating the values $f(1), f(2), \ldots$ from (36), successively, we obtain a function $f(n)$ satisfying all the equalities of (36) and, consequently, satisfying (35).

The theorem is thus proved. ☐

Equations (36) enable us to find the values $f(n)$ provided $F(1), F(2), \ldots, F(n)$ are known. There exists also a general formula for the function $f(n)$, namely

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \tag{37}$$

which can alternatively be written in the form

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) \tag{38}$$

or in the form

$$f(n) = \sum_{kl=n} \mu(k) F(l), \tag{39}$$

where the summation is over all the pairs k, l of the natural numbers for which $kl = n$.

In order to prove these formulae it is, of course, sufficient to prove that the function defined by (39) satisfies formula (35) for every nattural number n.

In fact, (39) implies that

$$\sum_{d|n} f(d) = \sum_{d|n}\sum_{kl=d} \mu(k)F(l) = \sum_{lk|n} \mu(k)F(l)$$

$$= \sum_{l|n} F(l) \sum_{k|n/l} \mu(k) = F(n)$$

because, by the properties of the function μ stated above, $\sum_{k|n/l} \mu(k)$ is different from zero (and thus equal to 1) only if $n/l = 1$, i.e. $l = n$.

In particular, for $F(1) = 1$ and $F(n) = 0$, $n = 2, 3, \ldots$, Theorem 6 implies that there exists precisely one function f, namely the Möbius function, $\mu(n) = f(n)$, for which the following conditions are satisfied,

$$f(1) = 1, \quad \sum_{d|n} f(d) = 0 \quad \text{for} \quad n = 2, 3, \ldots$$

11. The Liouville function $\lambda(n)$

This is the arthmetical function defined by the conditions

1° $\lambda(1) = 1$,

2° $\lambda(n) = (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_k}$ provided the factorization of n into prime numbers is of the form (1).

We have $\lambda(1) = 1$, $\lambda(2) = \lambda(3) = -1$, $\lambda(4) = 1$, $\lambda(5) = -1$, $\lambda(6) = 1$, $\lambda(7) = \lambda(8) = -1$, $\lambda(9) = \lambda(10) = 1$.

Suppose that for a natural number $n > 1$ the factorization of n into primes is as in (1).

Consider the product

$$\prod_{i=1}^{k} (1 - q_i^s + q_i^{2s} - q_i^{3s} + \ldots + (-1)^{\alpha_i} q_i^{\alpha_i s}),$$

where s is an arbitrary integer. Expanding this product, we obtain the algebraic sum of the summands $(q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k})^s$, each multiplied by $(-1)^{\lambda_1+\ldots+\lambda_k} = \lambda(q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k})$, where the summation is all over the set of the divisors $d = q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k}$ of the number n. Consequently, the product is equal to the sum $\sum_{d|n} \lambda(d) d^s$.

On the other hand, the formula for the sum of a geometric progression gives

$$1 - q_i^s + q_i^{2s} - q_i^{3s} + \ldots + (-1)^{\alpha_i} q_i^{\alpha_i s} = \frac{1 + (-1)^{\alpha_i} q_i^{(\alpha_i+1)s}}{1 + q_i^s}.$$

Applying this to each of the factors of the product we get

$$\prod_{i=1}^{k} \frac{1+(-1)^{\alpha_i} q_i^{(\alpha_i+1)s}}{1+q_i^s} = \sum_{d|n} \lambda(d)\, d^s.$$

In particular, for $s = 0$ we obtain the formula

$$\frac{1+(-1)^{\alpha_1}}{2} \cdot \frac{1+(-1)^{\alpha_2}}{2} \cdots \frac{1+(-1)^{\alpha_k}}{2} = \sum_{d|n} \lambda(d). \tag{40}$$

The number $\dfrac{1+(-1)^{\alpha}}{2}$ is equal to zero or to one, depending on whether α is odd or even. It follows that the left-hand side of formula (40) is different from zero, and thus equal to 1, if and only if all the exponents $\alpha_1, \alpha_2, \ldots, \alpha_k$ are even, i.e. if n is the square of a natural number. Thus we have proved the following

THEOREM 7. *The sum* $\sum_{d\backslash n} \lambda(d)$ *is equal either to* 0 *or—in the case where* n *is the square of a natural number—to* 1.

Although in the proof of Theorem 7 we assumed $n > 1$, the theorem is true for $n = 1$, since $\lambda(1) = 1$.

Let $F(n) = \sum_{d|n} \lambda(d)$. Consequently, $F(n) = 1$ holds for any n which is the square of a natural number and $F(n) = 0$ otherwise. In virtue of (30) (for $f(k) = \lambda(k)$) we obtain

$$\sum_{k=1}^{[x]} \lambda(k) \left[\frac{x}{k}\right] = \sum_{n=1}^{[x]} F(n)$$

whenever $x \geqslant 1$. The sum on the right-hand side of this equality consists of as many summands equal to 1 as there are natural numbers $\leqslant x$ which are squares. Consequently the sum is equal to $[\sqrt{x}]$. Hence

$$\sum_{k=1}^{[x]} \lambda(k) \left[\frac{x}{k}\right] = [\sqrt{x}] \quad \text{for} \quad x \geqslant 1.$$

CHAPTER V

CONGRUENCES

1. Congruences and their simplest properties

Let a and b be two integers. We say that *a is congruent to b with respect to the modulus m* if the difference of a and b is divisible by m. Using the notation introduced by Gauss, we write

$$a \equiv b \pmod{m}. \tag{1}$$

Thus formula (1) is equivalent to the formula

$$m \mid a-b.$$

It is clear that, if two integers are congruent with respect to the modulus m, then the division of either of them by m gives the same remainder and *vice versa*.

There is an analogy between congruence and *equality* (this justifies the use of the symbol $\equiv$, similar to the symbol of equality). We list here some of the more important properties which illustrate this analogy:

I. *Reflexivity* means that every integer is congruent to itself with respect to any modulus; i.e.

$$a \equiv a \pmod{m}$$

for any integer a and any natural number m. To prove this it is sufficient to observe that the number $a-a = 0$ is divisible by every natural number m.

II. *Symmetry* means that congruence (1) is equivalent to the congruence $b \equiv a \pmod{m}$. To prove this it is sufficient to note that the numbers $a-b$ and $b-a$ are either both divisible or both not divisible by a natural number m.

III. *Transitivity* means that, if

$$a \equiv b \pmod{m} \quad \text{and} \quad b \equiv c \pmod{m},$$

then

$$a \equiv c \pmod{m}.$$

To prove this we apply the identity

$$a-c = (a-b)+(b-c)$$

and recall the fact that the sum of two numbers, each of them divisible by m, is divisible by m.

Similarly, it is very easy to prove some other properties of congruence.

We prove that *two congruences can be added or subtracted from each other provided both have the same modulus.*

Let

$$a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m}. \tag{2}$$

In order to prove that $a+c \equiv b+d \pmod{m}$ and $a-c \equiv b-d \pmod{m}$ it is sufficient to apply the identities

$$(a+c)-(b+d) = (a-b)+(c-d) \quad \text{and} \quad (a-c)-(b-d) = (a-b)-(c-d).$$

Similarly, using the identity

$$ac-bd = (a-b)\,c+(c-d)\,b,$$

we prove that congruences (2) imply the congruence

$$ac \equiv bd \pmod{m}.$$

Consequently, we see that *two congruences having the same modulus can be multiplied by each other.*

The theorem on the addition, subtraction and multiplication of two congruences can easily be extended to the case of any finite number of congruences.

The theorem on addition of congruences implies that *the summands can be transferred, with the opposite sign,* in just the same way as in equations, *from one side of a congruence to the other.* This is because that operation is equivalent to the subtraction of the transferred summand from each side of the congruence.

It follows from the theorem on the multiplication of congruences that *a congruence can always be multiplied throughout by any integer and that each side of a congruence can be raised to the same natural power.*

But it is not always legitimate to divide one congruence by another (even if the quotients are integers). For example the congruences $48 \equiv 18 \pmod{10}$ and $12 \equiv 2 \pmod{10}$ do not imply the congruence $4 \equiv 9 \pmod{10}$.

It follows immediately from the theorem stating that a divisor of a divisor of an integer is a divisor of that integer that, if $d|m$, then *the congruence* $a \equiv b \pmod{m}$ *implies the congruence* $a \equiv b \pmod{d}$.

The law of transitivity of congruences together with the theorem on the addition and multiplication of congruences implies that *in a given* *congruence we can replace any summand or factor by any other, congruent to it.*

This rule is not valid for the exponents. For example the congruence $2^6 \equiv 4 \pmod 5$ cannot be replaced by the congruence $2^1 \equiv 4 \pmod 5$ though $6 \equiv 1 \pmod 5$.

Now, let

$$f(x) = A_0 x^n + A_1 x^{n-1} + \dots + A_{n-1} x + A_n$$

be a polynomial of the nth degree with integral coefficients. Let m be a natural modulus and a, b integers such that $a \equiv b \pmod m$. The theorems on the natural powers and on the multiplication of congruences justify the following sequence of congruences:

$$\begin{aligned} A_0 a^n &\equiv A_0 b^n \pmod m, \\ A_1 a^{n-1} &\equiv A_1 b^{n-1} \pmod m, \\ &\dots\dots\dots\dots\dots\dots \\ A_{n-1} a &\equiv A_{n-1} b \pmod m, \\ A_n &\equiv A_n \pmod m. \end{aligned}$$

Adding them up, we obtain

$$A_0 a^n + A_1 a^{n-1} + \dots + A_{n-1} a + A_n \\ \equiv A_0 b^n + A_1 b^{n-1} + \dots + A_{n-1} b + A_n \pmod m,$$

i.e. $f(a) \equiv f(b) \pmod m$. We have thus proved the following

THEOREM 1. *If $f(x)$ is a polynomial in x with integral coefficients, then the congruence $a \equiv b \pmod m$ implies the congruence $f(a) \equiv f(b) \pmod m$.*

An illustration of the use of Theorem 1 is provided by the rules of divisibility of a number by 9, 7, 11, 13, 27, 37.

Let N be a natural number. The usual representation of the number N by its digits in the scale of 10 is in fact a representation of N in the form

$$N = c_1 10^{n-1} + c_2 10^{n-2} + \dots + c_{n-1} 10 + c_n.$$

Let

(3) $$f(x) = c_1 x^{n-1} + c_2 x^{n-2} + \dots + c_{n-1} x + c_n.$$

Then $f(x)$ is a polynomial with integral coefficients and

(4) $$f(10) = N.$$

In virtue of Theorem 1, since $10 \equiv 1 \pmod 9$, we have

(5) $$f(10) \equiv f(1) \pmod 9.$$

But $f(1) = c_1 + c_2 + \ldots + c_n$ and, consequently, by (4) and (5),

$$N \equiv c_1 + c_2 + \ldots + c_n \pmod 9,$$

which proves that any natural number N differs from the sum of its digits (in the scale of 10) by a multiple of 9. In particular, *N is divisible by 9 if and only if the sum of its digits is divisible by 9.*

In general, if s_N denotes the sum of the digits of N (in the scale of 10), then for natural numbers N and N' we have

$$N \equiv s_N \pmod 9, \qquad N' \equiv s_{N'} \pmod 9,$$

whence $NN' \equiv s_N s_{N'} \pmod 9$. Since also $NN' \equiv s_{NN'} \pmod 9$, then $s_{NN'} \equiv s_N s_{N'} \pmod 9$. This relation between the sums of the digits of the factors and the sum of the digits of the product serves as the basis for the well-known *test of multiplication by the use of* 9.

By (3) and by the congruence $10 \equiv -1 \pmod{11}$, Theorem 1 implies that $f(10) \equiv f(-1) \pmod{11}$, whence, by (4) and (3), we obtain

$$(-1)^{n-1} N \equiv c_1 - c_2 + c_3 - c_4 + \ldots \pmod{11}.$$

This gives the rule of divisibility by 11.

Now we are going to find the rules of divisibility by 7 or 13. Denote by $(c_1 c_2 \ldots c_n)_{10}$ the number whose digits, in the scale of 10, are $c_1, c_2, \ldots, c_n$; this notation is really necessary in order to distinguish a number from the product of its digits $c_1 c_2 \ldots c_n$. Every natural number can be represented in the form

$$N = (c_{n-2}\, c_{n-1}\, c_n)_{10} + (c_{n-5}\, c_{n-4}\, c_{n-3})_{10} \cdot 1000 + \\ + (c_{n-8}\, c_{n-7}\, c_{n-6})_{10} \cdot 1000^2 + \ldots$$

Since $1000 \equiv -1 \pmod 7$ and $1000 \equiv -1 \pmod{13}$, we obtain the congruence

$$N \equiv (c_{n-2}\, c_{n-1}\, c_n)_{10} - (c_{n-5}\, c_{n-4}\, c_{n-3})_{10} + (c_{n-8}\, c_{n-7}\, c_{n-6})_{10} - \ldots \pmod 7$$

and a congruence identical to the above with the modulus 7 replaced by 13. These congruences give the rules of divisibility by 7 or 13. For example,

$$N = 8589879056 \equiv 56 - 879 + 589 - 8 \pmod 7 \text{ and } \pmod{13}.$$

Since the number on the right-hand side of these congruences, equal to -242, is divisible neither by 7 nor by 13, we see that the number N is not divisible by 7 or by 13.

The rules for 27 and 37 are based on the fact that

$$1000 \equiv 1 \pmod{27} \text{ and } \pmod{37}.$$

From this the rules are obtained in a complete analogy with the previous ones. For example, we have

$$N = 24540509 \equiv 509+540+24 \pmod{27} \text{ and } \pmod{37}.$$

The number on the right-hand side of this congruence is 1073. So we may write again $1073 \equiv 73+1 \pmod{27}$ and $\pmod{37}$. Number 74 is divisible by 37 but it is not divisible by 27, consequently the same is true about number N.

EXERCISES. **1.** Find the last two digits of the number 2^{1000}.

SOLUTION. We have $2^{10} = 1024 \equiv 24 \pmod{100}$. Hence $2^{20} \equiv 24^2 \equiv 76 \pmod{100}$. But $76^2 \equiv 76 \pmod{100}$, whence, by induction, $76^k \equiv 76 \pmod{100}$, $k = 1, 2, \ldots$ Therefore $2^{1000} = 2^{20 \cdot 50} \equiv 76^{50} \equiv 76 \pmod{100}$. Thus we see that the last two digits of number 2^{1000} are 7 and 6.

2. Prove that for an integer x at least one of the following six congruences is valid (cf. Erdős [10]): 1) $x \equiv 0 \pmod 2$, 2) $x \equiv 0 \pmod 3$, 3) $x \equiv 1 \pmod 4$, 4) $x \equiv 3 \pmod 8$, 5) $x \equiv 7 \pmod{12}$, 6) $x \equiv 23 \pmod{24}$.

PROOF. If an integer x satisfy neither 1) nor 2), then it is not divisible by 2 or by 3, and thus it is of the form $24t+r$, where t is an integer and r is one of the numbers 1, 5, 7, 11, 13, 17, 19, 23. Then, as can easily be verified, the number $x = 24t+r$ satisfies one of the congruences 3), 3), 5), 4), 3), 3), 4), 6). □

REMARK. P. Erdős [10] has proposed the following problem: given any natural number n, does there exist a finite set of congruences which uses only different moduli greater than n and such that every integer satisfies at least one of them? H. Davenport [2] conjectures that the answer is positive but, he says, it is not easy to see how to give a proof. P. Erdős himself has proved this for $n = 2$ (he has given the set of such congruences, the moduli being various factors of 120). D. Swift has given the proof for $n = 3$ (he has found the set of such congruences, the moduli being various factors of 2880). At present the conjecture is proved for $n < 20$ (see Choi [1]).

3. Find the last two digits of number 9^{9^9}.

SOLUTION. We easily find that with respect to the modulus 100 the following congruences hold

$$9^2 \equiv 81,\ 9^4 \equiv 81^2 \equiv 61,\ 9^8 \equiv 61^2 \equiv 21,\ 9^9 \equiv 21 \cdot 9 \equiv 89,\ 9^{10} \equiv 89 \cdot 9 \equiv 1.$$

We then have $9^9 \equiv 9 \pmod{10}$, whence $9^9 = 10k+9$, where k is a natural number. Hence, since $9^{10} \equiv 1 \pmod{100}$, it follows that $9^{9^9} = 9^{10k+9} \equiv 9^9 \equiv 89 \pmod{100}$, which proves that the last digit of number 9^{9^9} is 9 and the last but one is 8.

4. Find the last two digits of number $9^{9^{9^9}}$

SOLUTION. It follows from Exercise 3 that $9^{9^9} \equiv 9 \pmod{10}$. Consequently $9^{9^9} = 10t+9$, where t is a natural number, whence $9^{9^{9^9}} = 9^{10t+9} \equiv 9^9 \equiv 89 \pmod{100}$. Thus we see that the last two digits of number $9^{9^{9^9}}$ are identical with those of 9^{9^9}.

REMARK. According to W. Lietzmann [1], p. 118, the number of digits of this number has more than a quarter of a million digits.

Gauss is said to have called this number "a measurable infinity".

2. Roots of congruences. Complete set of residues

Let $f(x)$ be a polynomial of the nth degree with integral coefficients and let m be a given modulus. Any number a for which $f(a) \equiv 0 \pmod{m}$ is called a *root of the congruence*

$$f(x) \equiv 0 \pmod{m}. \tag{6}$$

If follows from Theorem 1 that if a is a root of congruence (6), then any number which is congruent to a with respect to the modulus m is also a root of (6). Therefore it is justified to regard the whole class of such roots as a single root of the congruence. This root can of course be represented by any number of this class.

Every integer is congruent with respect to modulus m to precisely one number of the sequence

$$0, 1, 2, \ldots, m-1. \tag{7}$$

In fact, let a be a given integer and let $r = a - m\left[\frac{a}{m}\right]$. Number r is an integer congruent to a with respect to m. Since $t-1 < [t] \leqslant t$ for real numbers t we have $\frac{a}{m} - 1 < \left[\frac{a}{m}\right] \leqslant \frac{a}{m}$, whence $0 \leqslant r < m$. Thus we see that number r belongs to sequence (7), and consequently every natural number a is congruent (with respect to m) to at least one of the numbers of sequence (7). Since, on the other hand, any two of the numbers of (7) give different remainders while divided by m, every integer a is congruent precisely to one of the numbers of (7). This number is called the *remainder* of number a with respect to modulus m.

All integers which are congruent to the same remainder r with respect to modulus m are of course of the form $mk+r$, where k is an integer and *vice versa*.

In order to solve congruence (6) (where $f(x)$ is a polynomial with integral coefficients) it is sufficient to find which of the numbers of sequence (7) are roots of the congruence. Thus we see that (6) can be solved by finitely many trials. This shows that, apart from the difficulties of a purely technical nature, we are able either to solve congruence (6) (where $f(x)$ is a polynomial with integral coefficients) or to prove that $f(x)$ has no roots.

EXAMPLES. 1. We solve the congruence

$$x^5 - 3x^2 + 2 \equiv 0 \pmod{7}. \tag{8}$$

We have to find which of the numbers 0, 1, 2, 3, 4, 5, 6 satisfies (8). Substituting 0 and 1 in (8), successively, we see that 1 is and 0 is not a solution of (8). Similarly, substituting 2, we see that 2 is not a solution of (8). For number 3 we may proceed as follows. We see that $3^2 \equiv 2 \pmod{7}$, whence $3^4 \equiv 4 \pmod{7}$ and $3^5 \equiv 12 \equiv 5 \pmod{7}$. Therefore $3^5-3\cdot 3^2+2 \equiv 5-3\cdot 2+2 \equiv 1 \pmod{7}$, and thus number 3 is not a solution of (8). For number 4 we have $4 \equiv -3 \pmod{7}$, whence $4^5 \equiv -3^5 \equiv -5 \pmod{7}$ and so $4^5-3\cdot 4^2+2 \equiv -5-3\cdot 2+2 \equiv 3 \pmod{7}$; consequently the number 4 is not a solution of (8) either. For number 5 we have $5 \equiv -2 \pmod{7}$, whence $5^5 \equiv -2^5 \equiv 3 \pmod{7}$ and $5^5-3\cdot 5^2+2 \equiv 3-3\cdot 4+2 \equiv 0 \pmod{7}$, and so number 5 is a solution of (8). For number 6 we have $6 \equiv -1 \pmod{7}$, whence $6^5-3\cdot 6^2+2 \equiv -1-3+2 \equiv 5 \pmod{7}$, and so 6 is not a solution of (8). We have thus shown that congruence (8) has two roots, 1 and 5. Therefore every integer x which satisfies congruence (8) is of the form $7k+1$ or $7k+5$, where k is an arbitrary integer.

2. We now solve the congruence

$$x^2+x \equiv 0 \pmod{2}. \tag{9}$$

Here the only thing that we have to do is to verify whether (9) is satisfied by numbers 0 and 1. We see that both of them satisfy the congruence (9), which proves that every integer x is a solution of (9). This also follows from the remark that numbers x^2 and x are always either both odd or both even, and so their sum is always even.

We say that a congruence which holds for every integer holds identically. The example presented above shows that for a congruence which holds identically the coefficients not necessarily all are divisible by the modulus.

Another example of a congruence which holds identically is the congruence $x^3-x \equiv 0 \pmod{3}$. In fact, $x^3-x = (x-1)x(x+1)$, whence, since of three consecutive integers one is divisible by 3, we deduce that $x^3-x \equiv 0 \pmod{3}$ for any integers x.

3. The fact that (9) holds identically implies that the congruence $x^2+x+1 \equiv 0 \pmod{2}$ has no solution. Similarly, the congruence $x^2 \equiv 3 \pmod{8}$ does not hold for any integer x, since the square of an odd integer yields the remainder 1, when divided by 8 while the remainder obtained from the division of the square of an even number by 8 is 0 or 4.

Let m denote a given modulus, k a given natural number $< m$ and $a_1, a_2, \ldots, a_k$ different non-negative integers $< m$. We ask whether there exists a polynomial $f(x)$ with integral coefficients such that the roots of the congruence $f(x) \equiv 0 \pmod{m}$ are precisely the numbers $a_1, a_2, \ldots, a_k$ (or numbers congruent to any of them with respect to m).

If m is a prime, then, clearly, the required function is $f(x) = (x-a_1) \times (x-a_2) \ldots (x-a_k)$. If $m = 4$ and $a_1, a_2, \ldots, a_k$, $k \leqslant 4$, are given nonnegative different integers < 4, then, as can easily be verified, the roots of the congruence $(x-a_1)(x-a_2)\ldots(x-a_k) \equiv 0 \pmod{4}$ are the numbers $a_1, a_2, \ldots, a_k$ (or numbers congruent to any of them with respect to 4). However, as has been proved by M. Chojnacka-Pniewska [1], there is no polynomial $f(x) = a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ for which the congruence $f(x) \equiv 0 \pmod{6}$ is satisfied by numbers 2 and 3 and not satisfied by any other integer < 6.

In fact, suppose that $f(x)$ is such a polynomial. Then $f(2) \equiv f(3) \equiv 0 \pmod{6}$, whence $3f(2)-2f(3) \equiv 0 \pmod{6}$. We have $3 \cdot 2^k \equiv 2 \cdot 3^k \equiv 0 \pmod{6}$ for any $k = 1, 2, \ldots$ Hence $3f(2) \equiv 3a_n \pmod{6}$ and $2f(3) \equiv 2a_n \pmod{6}$. Therefore $3f(2)-2f(3) \equiv a_n \pmod{6}$, whence $a_n \equiv 0 \pmod{6}$, so $f(0) \equiv 0 \pmod{6}$. We have thus proved that the congruence $f(x) \equiv 0 \pmod{6}$ has a root $x = 0$, contrary to the assumption that 2 and 3 are its only roots.

It can be proved (cf. Sierpiński [15]) that if m is a composite number $\neq 4$, then there exist two integers a and b which, divided by m, give a remainder different from zero and such that if $f(x)$ is a polynomial with integral coefficients, then the congruences $f(a) \equiv f(b) \equiv 0 \pmod{m}$ imply the congruence $f(0) \equiv 0 \pmod{m}$.

From this we easily deduce that if m is a composite number $\neq 4$, then there exists a polynomial of the second degree $f(x) = x^2 + a_1 x + a_2$ with integral coefficients for which the congruence $f(x) \equiv 0 \pmod{m}$ has more than two roots.

There is a close connection between congruences and a type of the Diophantine equations, namely equations which are linear with respect to one of the unknowns. In fact, in order that an integer x may satisfy congruence (6) it is necessary and sufficient that there should exist an integer y such that $f(x) = my$. Thus congruence $f(x) \equiv 0 \pmod{m}$ is equivalent to the Diophantine equation

$$f(x) - my = 0.$$

An argument analogous to that which we used in the case of the algebraic congruence of one unknown shows that if the left-hand side of a congruence is a polynomial in several variables with integral coefficients, then, if we do not take into account the difficulties of a purely technical nature, we are able to solve the congruence.

For example, in order to solve the congruence in two variables

$$f(x, y) \equiv 0 \pmod{m}$$

where $f(x, y)$ is a polynomial in variables x, y, it is sufficient to find which of the m^2 systems x, y with x and y ranging over the set of integers $0, 1, \ldots, m-1$, satisfy the congruence. (In fact, this follows easily from the remark that if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $f(a, b) \equiv f(c, d) \pmod{m}$).

A simple numerical example of what we have just said is provided by the congruence

$$x^4+y^4 \equiv 1 \pmod 5.$$

As we can verify directly it has 8 solutions: $(x, y) = (0, 1), (0, 2), (0, 3), (0, 4), (1, 0), (2, 0), (3, 0), (4, 0)$. Thus all the solutions of this congruence are the integers x, y such that one of them is divisible by 5 and the other is not.

It is also easy to see that the congruence

$$x^3+y^3+z^3 \equiv 4 \pmod 9$$

is insolvable. This is because the cube of an integer is congruent with respect to the modulus 9 to one of the numbers $0, 1, -1$, and so the sum of three cubes cannot be congruent to 4.

3. Roots of polynomials and roots of congruences

If an equation $f(x, y) = 0$, where $f(x, y)$ is a polynomial with the integral coefficients, has a solution in integers x, y, then, of course, for every natural number m there exist integers x, y such that the number $f(x, y)$ is divisible by m, i.e. such that the congruence $f(x, y) \equiv 0 \pmod m$ is solvable for each natural number m. Hence it follows that if there exists a modulus m such that the congruence $f(x, y) \equiv 0 \pmod m$ is not solvable in integers, then the equation $f(x, y) = 0$ has no solution in integers.

For example the proof that for natural numbers n the equation $x^2+1-3y^n = 0$ is insolvable in integers follows from the fact that the congruence $x^2+1-3y^n \equiv 0 \pmod 3$ has no solutions, this being a simple consequence of the fact that the square of an integer differs from the multiple of 3 either by 0 or by 1, whence the left-hand side of the congruence divided by 3 yields the remainder 1 or 2 but not 0.

It is not true, however, that for any polynomial $f(x, y)$ with integral coefficients for which the equation $f(x, y) = 0$ has no solutions in integers x, y there exists a modulus m such that the congruence $f(x, y) \equiv 0 \pmod m$ is insolvable.

For instance the equation

$$(2x-1)(3y-1) = 0$$

has no solutions in integers x, y; the congruence

$$(2x-1)(3y-1) \equiv 0 \pmod m,$$

however, is solvable for any natural number m. To see this we recall the well-known fact that a natural number m can be written in the form $m = 2^{k-1}(2x-1)$, where k, x are natural numbers. Number $2^{2k+1}+1$ is, as we know, divisible by $2+1 = 3$, and so there exists a natural number y

such that $2^{2k+1}+1 = 3y$. Consequently $(2x-1)(3y-1) = 2^{k+2}m$, which proves that the congruence under consideration is solvable.

It is easy to prove a stronger and more general assertion. If a_1, a_2 are two natural numbers such that $(a_1, a_2) = 1$, b_1, b_2 are arbitrary integers, then the congruence

$$(a_1 x+b_1)(a_2 y+b_2) \equiv 0 \pmod m$$

is solvable for every natural number m (cf. Skolem [1]).

It is easy to prove that the equation $2x^2-219y^2 = 1$ has no solution in integers x, y. This is because the congruence $2x^2-219y^2 \equiv 1 \pmod 3$ is insolvable. (In fact, if x is an integer, x^2 divided by 3 gives the remainder 0 or 1, and so, since $219 = 3\cdot 73$, number $2x^2-219y^2$ differs from a multiple of 3 by 0 or 2, and consequently it cannot be congruent to 1 with respect to modulus 3.)

It is a little more difficult to prove that the equation $2x^2-219y^2 = -1$ is insolvable in integers. T. Nagell [7] has deduced this from a more general theorem, the proof of which is difficult. However, the congruence $2x^2-219y^2 \equiv -1 \pmod m$ is, as he says (ibid. p. 62), easily proved to be solvable for any natural number m.

We present here a direct proof of the fact that the equation $2x^2-219y^2 = -1$ is insolvable in integers x, y.

Suppose, to the contrary, that the equation is solvable in integers x, y. Then, of course, neither of the numbers x, y can be zero, consequently, we may assume that x, y are positive integers. Moreover, we assume that the solution x, y is chosen in such a way that y is the least among the corresponding numbers in all the solutions of the equation in natural numbers. Let

$$x_1 = |293x-3066y|, \qquad y_1 = -28x+293y.$$

As is easy to verify, we have $2x_1^2-219y_1^2 = 2x^2-219y^2$. Consequently, the numbers x_1, y_1 satisfy the equation. We cannot have $x_1 = 0$, and so x_1 is a natural number. We cannot have $y_1 \leqslant 0$ either, since if we had, we would have $x \geqslant \frac{293}{28}y$, whence $x^2 \geqslant \frac{85849}{784}y^2$, and so $2x^2-219y^2 \geqslant \frac{y^2}{392}$, whence $-1 \geqslant \frac{y^2}{392}$, which is impossible. Thus we see that x_1, y_1 are natural numbers. By assumption, $y \leqslant y_1$, so $-28x+293y \geqslant y$, whence $x \leqslant \frac{292}{28}y = \frac{73}{7}y$, therefore $x^2 \leqslant \frac{5329}{49}y^2$ and $2x^2-219y^2 \leqslant \frac{-73}{49}y^2 \leqslant -\frac{73}{49} < -1$, contrary to the assumption that x, y is a solution of the equation. We have thus proved that the equation has no solutions in integers x, y.

We now prove that the congruence

$$2x^2-219y^2 \equiv -1 \pmod{m}$$

is solvable for any natural number m.

Let m be a natural number. We put $m = m_1 \cdot m_2$, where $m_1 = 11^\alpha$ (α is an integer $\geqslant 0$) and $(m_2, 11) = 1$. Let $x_1 = 5 \cdot 13^{\varphi(m_1)-1}$, $y_1 = 13^{\varphi(m_1)-1}$. Since $(13, m_1) = 1$, by the theorem of Euler (see Chapter VI, p. 261) $13^{\varphi(m_1)} \equiv 1 \pmod{m_1}$. Consequently,

$$\begin{aligned}13^2(2x_1^2-219y_1^2) = 2\cdot 25\cdot 13^{2\varphi(m_1)}-219\cdot 13^{2\varphi(m_1)} &\equiv 2\cdot 25-219\\ &\equiv -13^2 \pmod{m_1},\end{aligned}$$

whence, in virtue of the equality $(13, m_1) = 1$, we obtain $2x_1^2-219y_1^2 \equiv -1 \pmod{m_1}$.

Now let $x_2 = 7\cdot 11^{\varphi(m_2)-1}$, $y_2 = 11^{\varphi(m_2)-1}$. Since $(11, m_2) = 1$, we have $11^{\varphi(m_2)} \equiv 1 \pmod{m_2}$, whence

$$\begin{aligned}11^2(2x_2^2-219y_2^2) = 2\cdot 49\cdot 11^{2\varphi(m_2)}-219\cdot 11^{2\varphi(m_2)} &\equiv 2\cdot 49-219\\ &\equiv -11^2 \pmod{m_2}\end{aligned}$$

and so, by $(11, m_2) = 1$, we obtain $2x_2^2-219y_2^2 \equiv -1 \pmod{m_2}$. Now, since $(m_1, m_2) = 1$, in virtue of the Chinese remainder theorem (cf. Chapter I, § 12), there exist integers x, y such that

$$x \equiv x_1 \pmod{m_1}, \qquad x \equiv x_2 \pmod{m_2},$$

$$y \equiv y_1 \pmod{m_1}, \qquad y \equiv y_2 \pmod{m_2}.$$

Hence $2x^2-219y^2 \equiv 2x_1^2-219y_1^2 \equiv -1 \pmod{m_1}$ and $2x^2-219y^2 \equiv 2x_2^2-219y_2^2 \equiv -1 \pmod{m_2}$ and so, since $(m_1, m_2) = 1$ and $m = m_1 m_2$,

$$2x^2-219y^2 \equiv -1 \pmod{m},$$

which shows that the congruence is solvable for any natural number m.

We are going to solve another example of a congruence, this time a congruence whose left-hand side is not a polynomial. The congruence is

$$(*) \qquad 2^x \equiv x^2 \pmod{3}.$$

Since $2^2 \equiv 1 \pmod{3}$, we have $2^{x+2k} \equiv 2^x \pmod{3}$ for all non-negative integers x and $k = 0, 1, 2, \ldots$ Since $(x+3l)^2 \equiv x^2 \pmod{3}$ for any integers x, l, we see that if x is a solution of congruence $(*)$, then $x+6t$, $t = 0, 1, 2, \ldots$, is also a solution of $(*)$. Among the numbers 0, 1, 2, 3, 4, 5 only 2 and 4 are solutions of congruence $(*)$. Thus all the solution of the congruence are numbers $2+6t$ or $4+6t$, where $t = 0, 1, 2, \ldots$

REMARK. A number which is congruent to a solution of congruence (∗) with respect to its modulus may not be a solution of (∗), e.g. number 5.

4. Congruences of the first degree

Let

$$ax \equiv b \pmod{m}, \tag{10}$$

where m is a given modulus and a, b are given integers. As we have learned in § 2, congruence (10) is equivalent to the Diophantine equation

$$ax - my = b. \tag{11}$$

It follows from Theorem 15 of Chapter I that in order that equation (11) be solvable in integers x, y, it is necessary and sufficient that $(a, m)|b$. Consequently, this is also a necessary and sufficient condition for solvability of congruence (10).

Suppose now that this condition is satisfied. We are going to look for the method of finding both all the solutions of congruence (10) and their number. Let $d = (a, m)$. So the number b/d is an integer. Let x_0 be one of the solutions of congruence (10) and let x be an arbitrary solution of it. We have $ax_0 \equiv b \pmod{m}$ and, by (10), we see that $a(x-x_0) \equiv 0 \pmod{m}$. Consequently, $m|a(x-x_0)$, whence $\frac{m}{d} \Big| \frac{a}{d}(x-x_0)$. But since, in virtue of $d = (a, m)$, the relation $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$ holds, $\frac{m}{d}$ must divide $x-x_0$, whence $x = x_0 + \frac{m}{d}t$, where t is an integer.

Conversely, taking an arbitrary integer for t and an arbitrary root x_0 of congruence (10) and putting $x = x_0 + \frac{m}{d}t$, we obtain a root of congruence (10), since $ax = ax_0 + \frac{a}{d}tm \equiv ax_0 \equiv b \pmod{m}$.

Now, let t take the values $0, 1, 2, \ldots, d-1$, successively. We prove that no two among the numbers

$$x_t = x_0 + \frac{m}{d}t \tag{12}$$

are congruent to one another with respect to the modulus m.

In fact, if $x_t \equiv x_u \pmod{m}$, then by (12) we would have $x_0 + \frac{m}{d}t \equiv x_0 + \frac{m}{d}u \pmod{m}$ and consequently $\frac{m}{d}(t-u) = mz$, where z is an integer, whence $t-u = dz$, which is impossible whenever t, u are different numbers of the sequence $0, 1, 2, \dots, d-1$.

Finally, we show that each root of congruence (10) is congruent with respect to the modulus m to one of the roots $x_0, x_1, \dots, x_{d-1}$ (defined in (12)).

In fact, if x is a root of congruence (10), then for an integer t we have $x = x_0 + \frac{m}{d}t$. Let r be the remainder obtained by dividing t by d. (So r is one of the numbers $0, 1, 2, \dots d-1$.) We have $t = r+du$, where u is an integer. Hence $x = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(r+du) = x_0 + \frac{m}{d}r + mu = x_r + mu$, whence $x \equiv x_r \pmod{m}$, as we have to prove.

Putting together the results just proved we obtain

THEOREM 2. *A congruence of the first degree* $ax \equiv b \pmod{m}$ *is solvable if and only if* b *is divisible by the greatest common divisor* d *of the coefficient of* x *and the modulus* m. *If this condition is satisfied, then the congruence has precisely* d *roots non-congruent with respect to the modulus* m.

In particular, if a and m are relatively prime numbers, then $d = 1$. Hence the following.

COROLLARY. *If the coefficient of* x *is relatively prime to the modulus* m, *then the congruence of the first degree* $ax \equiv b \pmod{m}$ *has precisely one root.*

If a congruence $ax \equiv b \pmod{m}$ is solvable and if $(a, m) = d > 1$, then another congruence is obtained from it, namely

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\,\frac{m}{d}\right), \quad \text{where} \quad \left(\frac{a}{d}, \frac{m}{d}\right) = 1.$$

Therefore, while solving a congruence of the first degree (in case the congruence is solvable), we may always assume that the coefficient at the unknown and the modulus are relatively prime.

C. Sardi [1] has given the following method for solving such congruences. Let $ax \equiv b \pmod{m}$, where $a > 1$ and $(a, m) = 1$. Further, let $a_1 = m-a\left[\frac{m}{a}\right]$; clearly $0 < a_1 < a$, since m is not divisible by a. Hence multiplying the congruence by $-\left[\frac{m}{a}\right]$ throughout we obtain $a_1x \equiv -b\left[\frac{m}{a}\right] \pmod{m}$, i.e. a congruence in which $a_1 < a$. Proceeding in this way, we ultimately obtain $a_n = 1$, i.e. the congruence $x \equiv c \pmod{m}$ whose unique solution is clearly $x = c$.

5. Wilson's theorem and the simple theorem of Fermat

Let p be an odd prime and D an integer not divisible by p.

Any two numbers m, n of the sequence

$$1, 2, 3, \ldots, p-1 \tag{13}$$

are called *corresponding* if and only if the congruence

$$mn \equiv D \pmod{p} \tag{14}$$

holds. If follows immediately from the definition that, if m is a number corresponding to n, then n is a number corresponding to m.

We now prove that for each number of sequence (13) there is precisely one number corresponding to it. Let m be a number of sequence (13). In order that a number x of sequence (13) may be a corresponding number to m it is necessary and sufficient that the congruence $mx \equiv D \pmod{p}$ should hold. In virtue of the relation $mx \equiv D \pmod{p}$ (where m is a number of sequence (13)) and in accordance with the corollary to Theorem 2, the last congruence has precisely one root. Therefore we see that in the sequence $0, 1, 2, 3, \ldots, p-1$ there is one and only one number which satisfies the congruence. It cannot be the number 0, since D is not divisible by p. From this we infer that in sequence (13) there is precisely one number which satisfies the congruence, as we were to show.

It may happen that corresponding numbers are equal. Then congruence (14) assumes the form $m^2 \equiv D \pmod{p}$. This is possible only if there exists a square which differs from D by a multiple of p; the number D is then called a *quadratic residue* for the modulus p. In the opposite case, that is, if none of the squares is congruent to D with respect to the modulus p, we say that D is a *quadratic nonresidue* for p. In other words, a number D not divisible by p is called a quadratic residue or a quadratic non-residue depending on whether the congruence $x^2 \equiv D \pmod p$ is solvable or insolvable.

First we consider the case where D is a quadratic non-residue for a prime modulus p. Then each pair of corresponding numbers m, n consists of two different numbers of sequence (13). Therefore all the numbers of sequence (13) can be divided into pairs of corresponding numbers, the number of the pairs being equal to $(p-1)/2$. Writing down the congruence of the form (14) for each of the pairs we obtain the sequence of $(p-1)/2$ congruences

$$\begin{aligned} m_1\, n_1 &\equiv D \pmod p, \\ m_2\, n_2 &\equiv D \pmod p, \\ &\cdots\cdots\cdots\cdots \\ m_{\frac{p-1}{2}}\, n_{\frac{p-1}{2}} &\equiv D \pmod p. \end{aligned}$$

Then multiplying these congruences and noting that the product $m_1\, n_1\, m_2\, n_2 \ldots m_{\frac{p-1}{2}}\, n_{\frac{p-1}{2}}$ differs from the product of the numbers of sequence (13) at most in the order of the factors, we obtain the congruence

$$(p-1)! \equiv D^{\frac{1}{2}(p-1)} \pmod p. \tag{15}$$

Now we consider the case where D is a quadratic residue for the modulus p. Then the congruence

$$x^2 \equiv D \pmod p \tag{16}$$

is solvable. Let us calculate the number of the numbers of (13) which satisfy congruence (16). Since we have assumed that congruence (16) is solvable, in the sequence $0, 1, 2, \ldots, p-1$ there is at least one number k which is a solution of (16). It cannot be $k = 0$, since, according to our general assumption, D is not divisible by p. Consequently the number k is one of the numbers of sequence (13) and therefore $p-k$ is also a number of this sequence. It is different from k, since, as we have assumed, p is an odd number. For the number $l = p-k$ we have $l^2 \equiv k^2 \pmod p$, whence the congruence $k^2 \equiv D \pmod p$ implies $l^2 \equiv D \pmod p$.

Thus in the case where D is a quadratic residue for p we see that in sequence (13) there are at least two different numbers which satisfy congruence (16). We prove that there are precisely two such numbers.

Suppose that a number x of sequence (13) satisfies congruence (16). Since $k^2 \equiv D \pmod p$, we have $x^2 \equiv k^2 \pmod p$, which proves that $p \mid x^2$

$-k^2 = (x-k)(x+k)$. But, since p is a prime number, that last relation implies that either $p|x-k$ or $p|x+k$. If $p|x-k$, then, since x and k belong to sequence (13), we see that $x = k$. If $p|x+k$, then, since $0 < x < p$ and $0 < k < p$ and so $0 < x+k < 2p$, we see that $x+k = p$, whence $x = p-k = l$.

We have thus proved that k and l are the only numbers of sequence (13) which satisfy congruence (16). Hence, *if a number D which is not divisible by an odd prime p is a quadratic residue for the modulus p, then congruence* (16) *has precisely two roots.*

Now we remove the numbers k and l from sequence (13). None of the remaining $p-3$ numbers satisfies congruence (16), so they can be divided into $(p-3)/2$ pairs of corresponding numbers. We thus obtain $(p-3)/2$ congruences

$$\begin{aligned} m_1 n_1 &\equiv D \pmod{p}, \\ m_2 n_2 &\equiv D \pmod{p}, \\ &\dots\dots\dots\dots\dots \\ m_{\frac{p-3}{2}} n_{\frac{p-3}{2}} &\equiv D \pmod{p}. \end{aligned}$$

Since $kl = k(p-k) \equiv -k^2 \equiv -D \pmod{p}$, we may add the congruence

$$kl \equiv -D \pmod{p}$$

to the congruences above and multiply all the congruences. Then the product of the left-hand sides of the congruences is equal to $(p-1)!$. Thus the congruence

$$(17) \qquad (p-1)! \equiv -D^{\frac{1}{2}(p-1)} \pmod{p}$$

is obtained.

We see that either (15) or (17) holds depending on whether D is a quadratic residue for the modulus p or not.

Putting together (15) and (17), we write

$$(18) \qquad (p-1)! \equiv \pm D^{\frac{1}{2}(p-1)} \pmod{p},$$

where on the right-hand side the sign $-$ or $+$ is taken, depending on whether D is a quadratic residue for p or not.

In particular, for $D = 1$ we see that, since number 1 is a quadratic residue for every p,

$$(19) \qquad (p-1)! \equiv -1 \pmod{p}.$$

The proof of (19) makes use of the assumption that p is an odd prime number and it fails for $p = 2$, but we can immediately verify that the result is still true since $(2-1)! = 1 \equiv -1 \pmod 2$. Thus we have proved the following.

THEOREM 3 (Wilson). *If p is a prime number, then the number $(p-1)!+1$ is divisible by p.*

The converse is also true. In fact, if p is a natural number > 1 and if $(p-1)!+1$ is divisible by p, then p is a prime. To see this we suppose to the contrary that p is not a prime. Then there is a divisor q of p such that $1 < q < p$. The number $(p-1)!+1$, being divisible by p, must also be divisible by q, but since $q < p$, $q \leqslant p-1$, so $q|(p-1)!$, whence $q|1$, which is a contradiction. Hence

THEOREM 3^a. *A necessary and sufficient condition for a natural number $n > 1$ to be a prime is that the number $(n-1)!+1$ is divisible by n.*

This shows that, from a purely theoretical point of view, we are able to decide for a given natural number $n > 1$ whether it is a prime or not using only one division.

It follows from Theorem 3 that for a prime p the number $w_p = \{(p-1)!+1\}/p$ is a natural number. C.E. Fröberg [2] has calculated the remainders obtained by dividing w_p by p for the prime numbers $p < 50000$. The primes for which $p^2|(p-1)!+1$ are called *Wilson primes*. It follows from the tables given by Fröberg that among the primes $p < 50000$ there are only three Wilson primes, namely 5, 13 and 563.

From Theorem 3^a and the remark that for $n > 2$ the relations $(n-1)! = (n-2)!\,(n-1) \equiv -(n-2)! \pmod n$ hold we deduce

THEOREM 3^b (Leibniz). *In order that a natural number $n > 1$ be prime it is necessary and sufficient that $(n-2)! \equiv 1 \pmod n$.* (By 0! we understand of course number 1.)

It can be proved that *a natural number $p > 1$ is a prime if and only if there exists a natural number $n < p$ such that $(n-1)!\,(p-n)! \equiv (-1)^n \pmod p$* (cf. Dickson [7], vol. I, p. 64).

It is clear that if n is a natural number such that $n|(n-1)!$, then n is a composite number. It is easy to prove that if n is a composite number $\neq 4$, then $n|(n-1)!$

In fact, if n is a composite number, then there exist natural numbers a and b such that $n = ab$, $1 < a < n$, $1 < b < n$. If $a \neq b$, then a and b are different factors of the product $(n-1)!$ and, consequently, $n = ab$ divides $(n-1)!$. If $a = b$, then $n = a^2$ and, since n is a composite number $\neq 4$, $a > 2$. Hence it follows that $n = a^2 \neq 2a$ and therefore a and $2a$ are different factors of the product $(n-1)!$. Thus $(n-1)!$ is divisible by $2a^2$, whence, *a fortiori*, it is divisible by $a^2 = n$. For $n = 4$, however, we have $(n-1)! = 3! = 6 \equiv 2 \pmod 4$.

It follows immediately from Theorem 3 that *there exist infinitely many natural numbers n for which $n!+1$ is a composite number*. Such are for instance the numbers $n = p-1$, where p is a prime > 3. (For, $(p-1)! > 2(p-1) = p+(p-2) > p$.)

A. Schinzel [14] has proved that for every rational $c \neq 0$ there exist infinitely many composite integers of the form $cn!+1$.

We do not know, however, whether there exist infinitely many prime numbers of the form $n!+1$. For $n < 546$ the only prime numbers of this form correspond to $n = 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427$ (see Buhler, Crandall and Penk [1]).

It is not known whether there exist infinitely many natural numbers k such that the number $P_k = p_1 p_2 \dots p_k + 1$ is a prime. Neither is it known whether there exist infinitely many k's for which P_k is composite. The following five numbers P_k are prime: $P_1 = 3$, $P_2 = 7$, $P_3 = 31$, $P_4 = 211$, $P_5 = 2311$, but $P_6 = 59 \cdot 509$, $P_7 = 19 \cdot 97 \cdot 277$, $P_8 = 347 \cdot 27953$, $P_9 = 317 \cdot 703763$, $P_{10} = 331 \cdot 571 \cdot 34231$ are not prime. For k between 10 and 442 the only primes P_k correspond to $k = 11, 75, 171, 172, 284$ (Buhler, Crandall and Penk [1]).

It follows from Theorem 3^b that *there exist infinitely many natural numbers n such that the number $n!-1$ is composite*. Such are, for instance, all the numbers $n = p-2$, where p is a prime > 5. We do not know whether there exist infinitely many primes of this form. If $n < 546$, numbers $n!-1$ are prime only for $n = 3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 427$ (Buhler, Crandall and Penk [1]).

Formulae (15) and (17) together with Theorem 3 give

THEOREM 4. *If an integer D is not divisible by an odd prime p, then*

$$D^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod p, \tag{20}$$

where the sign $+$ or $-$ is taken depending on whether D is a quadratic residue for the modulus p or not.

Hence, raising each side of (20) to the second power, we obtain

THEOREM 5. *If an integer D is not divisible by a prime p, then*

$$D^{p-1} \equiv 1 \pmod{p}. \tag{21}$$

This is the *simple theorem of Fermat*, given by him without a proof in 1640. The first proof was given by L. Euler in 1736.

The proof of formula (20) fails if $p = 2$, but we can immediately verify that (21) still holds; for D, being non-divisible by $p = 2$, must be odd, and so $D \equiv 1 \pmod{2}$.

In particular, it follows from Theorem 5 that, if p is an odd prime, then the number $2^{p-1}-1$ is divisible by p. Investigations have been made in order to find the numbers p for which $2^{p-1}-1$ is divisible by p^2. For $p < 6\cdot 10^9$ only two such numbers have been found, namely $p = 1093$, $p = 3511$. (Brillhart, Tonascia and Weinberger [1] and Lehmer [9]).

A simple application of Theorem 5 gives a solution of any congruence of the form $ax \equiv b \pmod{p}$ provided p is a prime and a is not divisible by p. In fact, $x = a^{p-2}b$ is a solution because, by Theorem 5, $a^{p-1} \equiv 1 \pmod{p}$, whence $ax = a^{p-1}b \equiv b \pmod{p}$.

An immediate consequence of Theorem 5 is

THEOREM 5^a. *If p is a prime number, then for every integer a we have $p|a^p-a$.*

Conversely, Theorem 5 can easily be obtained from Theorem 5^a. In fact, if a is an integer not divisible by a prime p, then the relation $p|a^p-a = a(a^{p-1}-1)$ implies $p|a^{p-1}-1$, that is $a^{p-1} \equiv 1 \pmod{p}$.

The theorems of Wilson and Fermat can be formulated together in a single theorem (cf. Moser [4]):

THEOREM 6. *If p is a prime and a an integer, then*

$$p|a^p+(p-1)!\,a. \tag{22}$$

In fact, if Theorem 3 holds, then $(p-1)! \equiv -1 \pmod{p}$, consequently, $a^p+(p-1)!\,a \equiv a^p-a \pmod{p}$, which, in virtue of Theorem 5^a, gives $a^p-a \equiv 0 \pmod{p}$, whence formula (22) follows.

On the other hand, if Theorem 6 holds, then for $a = 1$ formula (22) gives Theorem 3. Therefore for every integer a the congruence $a^p+(p-1)!\,a \equiv a^p-a \pmod{p}$ holds, whence it follows that (22) implies $a^p-a \equiv 0 \pmod{p}$. So Theorem 5^a is valid, and this, as we know, is equivalent to the theorem of Fermat.

It is also easy to prove that the theorems of Fermat and of Wilson taken together are equivalent to the following

THEOREM 6^a. *If p is a prime and a is an integer, then*

$$p \mid (p-1)!a^p + a.$$

In this connection we wish to add that several authors (cf. Dickson [7], Vol. 1, pp. 84–86 and T. Szele [1]) proved the following generalization of Theorem 5^a, first stated by J.A. Serret in 1855.

For every natural number m and every integer a the number $\sum_{d \mid m} \mu(d) a^{m/d}$ is divisible by m.

Hence, in particular, for each integer a and two different primes p and q we have $pq \mid a^{pq} - a^p - a^q + a$.

We derive another simple corollary from Theorem 5:

THEOREM 7. *There exist infinitely many prime numbers of the form $4k+1$ (where k is a natural number).*

PROOF. Let n be an arbitrary natural number > 1 and let

$$N = (n!)^2 + 1. \tag{23}$$

Number N is, of course, odd and > 1. Let p denote the least prime divisor of the number N. By (23), $p > n$. Being odd, p is of the form $4k+1$ or $4k+3$. By (23) again, we have

$$(n!)^2 \equiv -1 \pmod{p},$$

whence, raising each side of the congruence to the $(p-1)/2$-th power, we obtain $(n!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}$. But $n!$ is not divisible by p, and so, in view of Theorem 5, we have $(n!)^{p-1} \equiv 1 \pmod{p}$, whence

$$(-1)^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}. \tag{24}$$

We cannot have $p = 4k+3$ because, if we could, formula (24) would give

$$(-1)^{\frac{1}{2}(p-1)} = (-1)^{2k+1} = -1 \equiv 1 \pmod{p},$$

whence $p \mid 2$, which is impossible. Therefore p must be of the form $4k+1$.

We have thus proved that for every natural number $n > 1$ there exists a prime $p > n$ of the form $4k+1$. (More precisely, we have proved that such is every prime divisor of number (23)). Theorem 7 is thus proved. □

As far as the numbers $4k+3$ are concerned, it is very easy indeed to prove that there are infinitely many primes among them. In fact, let n denote an arbitrary natural number > 3 and let

$$N_1 = n!-1. \tag{25}$$

N_1 is an odd number > 1, and so each of its prime factors is odd. If each of them is of the form $4k+1$, then number N_1, as the product of (not necessarily different) numbers of the form $4k+1$, is itself of the form $4t+1$. But this, in view of (25) and the fact that $n > 3$, is impossible.

Thus we have proved that for every natural number $n > 3$ there exists a prime number $p > n$ of the form $4k+3$. Hence

THEOREM 7ª. *There are infinitely many primes of the form* $4k+3$ (*where k is a natural number*).

For a given real number $x > 1$ denote by $\pi_1(x)$ the number of primes $\leqslant x$ of the form $4k+1$; by $\pi_3(x)$ denote the number of primes $\leqslant x$ of the form $4k+3$. Let $\Delta(x) = \pi_3(x)-\pi_1(x)$. In 1914 J.E. Littlewood proved that there exist infinitely many natural numbers n such that $\Delta(n) > 0$ and that there are infinitely many n for which $\Delta(n) < 0$. It seems curious that until 1957 none of the numbers n for which $\Delta(n) < 0$ were known. With the aid of the electronic computer EDSAC, J. Leech [1] has calculated the numbers $\Delta(n)$ with $n \leqslant 3000000$. Thus he has shown that the least natural number n for which $\Delta(n) < 0$ is $n = 26861$. For this n we have $\pi_1(n) = 1473$, $\pi_3(n) = 1472$, and so $\Delta(n) = -1$. It has been found that $\Delta(623681) = -8$, $\Delta(627859) = \Delta(627860) = \ldots = \Delta(627900) = 0$, $\Delta(2951071) = 256$.

It follows from Theorem 5 that if p is a prime number, then $a^{p-1} \equiv 1 \pmod{p}$, where $a = 1, 2, \ldots, p-1$. Adding up these $p-1$ congruences, we obtain

$$1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1} \equiv p-1 \pmod{p}.$$

Hence

$$p \mid 1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1}+1$$

for any prime p. G. Giuga [1] has conjectured that this relation does not hold for composite numbers and E. Bedocchi [1](¹) proved this for $p \leqslant 10^{1700}$.

The theorem, which follows, is a corollary to Theorem 3.

(¹) See Bibliography, added in proof. p. 504.

THEOREM 8. *If p is a prime of the form $4k+1$ (where k is a natural number), then*

$$(26)\qquad p \,\Big|\, \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1.$$

PROOF. Since $\frac{1}{2}(p-1) = 2k$, we have the equality $1 \cdot 2 \cdot 3 \ldots \frac{1}{2}(p-1)$ $= (-1)(-2)\ldots\left(-\frac{p-1}{2}\right) \equiv (p-1)(p-2)\ldots\frac{p+1}{2} \pmod{p}$; hence we obtain

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \cdot 2 \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \ldots (p-1) \equiv (p-1)! \equiv -1 \pmod{p},$$

and this gives formula (26).

On the basis of Theorem 8 we prove the following

THEOREM 9 (Fermat). *Every prime number p of the form $4k+1$ is a sum of two squares.*

PROOF. Let p be a prime number of the form $4k+1$ and $a = \left(\frac{p-1}{2}\right)!$. In virtue of Theorem 8, we have $p \mid a^2+1$, a being of course relatively prime to p. In view of the theorem of Thue (cf. Chapter I, § 13) with p in place of m, there exist two natural numbers x, y, each $\leqslant \sqrt{p}$, such that for a suitable choice of the sign $+$ or $-$ the number $ax \pm y$ is divisible by p. Hence it follows that the number $a^2x^2 - y^2 = (ax-y)(ax+y)$ is divisible by p.

$a^2x^2 + x^2 = (a^2+1)x^2$ is divisible by p (since $p \mid a^2+1$). Consequently the number $x^2+y^2 = a^2x^2 + x^2 - (a^2x^2 - y^2)$ is divisible by p. But, since x, y are natural numbers $\leqslant \sqrt{p}$, they are $< \sqrt{p}$, because p, being a prime, is not a square of a natural number. Thus x^2+y^2 is a natural number > 1 and $< 2p$ and, moreover, it is divisible by p, so it must be equal to p, i.e. $p = x^2+y^2$. This proves that p is the sum of two squares of natural numbers. □

A number which is of the form $4k+3$ (not necessarily prime) can not be the sum of two squares. The argument is that, since the square of an integer is congruent to 0 or 1 (mod 4), the sum of any two squares must be congruent to 0, 1 or 2 but never to 3. This shows that among prime numbers only the number $2 = 1^2+1^2$ and the primes of the form $4k+1$ are the sums of two squares.

According to H. Davenport [2] (pp. 120–122) four constructions for the decomposition of a prime of the form $4k+1$ are known. They are due to Legendre (1808), Gauss (1825), Serret (1848) and Jacobsthal (1906), respectively. The most elementary of them all (to formulate though not to prove) is the following construction, due to Gauss. If $p = 4k+1$ is a prime number, we take integers x, y such that

$$x \equiv (2k)!/2(k!)^2 \pmod{p} \qquad \text{and} \qquad y \equiv (2k)!x \pmod{p},$$

with $|x| < \frac{1}{2}p$, $|y| < \frac{1}{2}p$. Then $p = x^2+y^2$. A proof has been given by Cauchy and another by Jacobsthal, but neither of them is simple. The calculation which leads to the numbers x, y is not easy. To illustrate this, take $p = 29$. Then $x \equiv 14!/2\cdot(7!)^2 = 1716 \equiv 5 \pmod{29}$, $y \equiv 14!x \equiv 14!\cdot 5 \equiv 2 \pmod{29}$, whence $x = 5$, $y = 2$.

We do not know whether there exist infinitely many primes p such that $p = x^2+(x+1)^2$, where x is a natural number. A positive answer follows from Conjecture H (cf. Chapter III, § 8). For example, we have $5 = 1^2+2^2$, $13 = 2^2+3^2$, $41 = 4^2+5^2$, $61 = 5^2+6^2$, $113 = 7^2+8^2$, $181 = 9^2+10^2$, $313 = 12^2+13^2$, $421 = 14^2+15^2$, $613 = 17^2+18^2$, $761 = 19^2+20^2$.

As can easily be observed, the conjecture that there exist infinitely many primes, each of them being the sum of two consecutive squares, is equivalent to the conjecture that there exist infinitely many primes p for which $2p = a^2+1$, where a is a natural number. To see this we suppose $p = x^2+(x+1)^2$, where x is a natural number, then $2p = (2x+1)^2+1$. Conversely, if $2p = a^2+1$, where a is a natural number, then, for $p > 2$, the number a must be odd > 1, and so $a = 2x+1$, where x is a natural number. Hence $2p = (2x+1)^2+1$, that is, $p = x^2+(x+1)^2$.

It follows from Conjecture H that there exist infinitely many primes p such that $p = a^2+b^2$, where a and b are prime numbers. For example, $13 = 2^2+3^2$, $29 = 2^2+5^2$, $53 = 2^2+7^2$, $173 = 2^2+13^2$, $293 = 2^2+17^2$, $1373 = 2^2+37^2$.

It also follows from Conjecture H that there exist infinitely many primes, each of them being the sum of three consecutive squares of natural numbers. For example, $29 = 2^2+3^2+4^2$, $149 = 6^2+7^2+8^2$, $509 = 12^2+13^2+14^2$, $677 = 14^2+15^2+16^2$, $1877 = 24^2+25^2+26^2$. In this connection, we note that conjecture H implies that there exist infinitely many prime numbers, each of them being the sum of three different squares of prime numbers. For example, $83 = 3^2+5^2+7^2$, 179

$= 3^2+7^2+11^2$, $419 = 3^2+11^2+17^2$, $563 = 3^2+5^2+23^2$. (It is easy to prove that one of the squares must always be equal to 3^2.)

Another corollary which can be derived from Conjecture H is that for every natural number n there exist infinitely many natural numbers x such that x^2+n^2 are primes.

It can be proved that for every natural number n there exists a prime p such that $p = a^2+b^2$ with $a > n$ and $b > n$ (cf. Chapter III, § 7, and the papers quoted there).

If a prime number is the sum of two or four squares of different prime numbers, then, as can easily be verified, one of the primes must be equal to 2. If a prime is the sum of three squares of different primes, then one of the primes must be equal to 3. However, it follows from Conjecture H that for every natural number n there exists a prime $q > p_{n+3}$ such that the number $p = p_n^2+p_{n+1}^2+p_{n+2}^2+p_{n+3}^2+q^2$ is a prime. For example, we have $373 = 3^2+5^2+7^2+11^2+13^2$, $653 = 5^2+7^2+11^2+13^2+17^2$, $1997 = 7^2+11^2+13^2+17^2+37^2$.

We now prove that the decomposition of a prime into the sum of two squares of natural numbers, if it exists, is unique apart from the order of the summands. We prove a slightly more general

THEOREM 10. *If a and b are natural numbers, then the representation of a prime p in the form $p = ax^2+by^2$, where x, y are natural numbers, if it exists, is unique, apart from the obvious possibility of interchanging x and y in the case of $a = b = 1$.*

PROOF. Suppose that for a prime p

$$p = ax^2+by^2 = ax_1^2+by_1^2, \tag{27}$$

where x, y, x_1, y_1 are natural numbers. Clearly, $(x, y) = (x_1, y_1) = 1$. From (27) we have

$$p^2 = (axx_1+byy_1)^2+ab(xy_1-yx_1)^2 = (axx_1-byy_1)^2+ab(xy_1+yx_1)^2.$$

But

$$\begin{aligned}(axx_1+byy_1)(xy_1+yx_1) &= (ax^2+by^2)x_1y_1+(ax_1^2+by_1^2)xy\\ &= p(x_1y_1+xy).\end{aligned}$$

Consequently at least one of the factors on the left-hand side of this equality must be divisible by p. If $p \mid axx_1+byy_1$, then the first of the above formulae for p^2 gives $xy_1-yx_1 = 0$. Therefore $x/y = x_1/y_1$, which, in view of $(x, y) = (x_1, y_1) = 1$, proves that $x = x_1$, $y = y_1$. If $p \mid xy_1+yx_1$, then the second of the formulae above for p^2 shows that

$p^2 \geqslant abp^2$, which is possible only in the case of $a = b = 1$. But then $xx_1 - yy_1 = 0$, and so $x/y = y_1/x_1$, which, in virtue of $(x, y) = (x_1, y_1) = 1$, shows that $x = y_1, y = x_1$. Then the decompositions $p = x^2 + y^2$ and $p = x_1^2 + y_1^2$ differ only in the order of the summands. Theorem 10 is thus proved. □

An immediate corollary to Theorem 10 is that if a natural number admits two (or more) different representations in the form $ax^2 + by^2$, where x, y are natural numbers, then it must be composite. The converse theorem is not true. Namely number 14 has a unique representation in the form $14 = 2x^2 + 3y^2$, where x, y are natural numbers ($x = 1, y = 2$) and the number 15, though composite, has no representation in the form $15 = 2x^2 + 3y^2$, where x, y are integers. Number 18 has a unique representation in the form $18 = x^2 + y^2$, where x, y are natural numbers (namely $x = y = 3$). Each of the numbers 25 and 45 has a unique representation (apart from the order of the summands) in the form $x^2 + y^2$, where x, y are natural numbers, namely $25 = 3^2 + 4^2$, $45 = 3^2 + 6^2$.

However, the following theorem holds:

THEOREM 11. *A natural number of the form* $4k + 1 > 1$ *is a prime if and only if it admits a unique representation (apart from the order of the summands) as the sum of two squares of integers* $\geqslant 0$ *and in this unique representation the squares are relatively prime.*

PROOF. Suppose that the number $p = 4k + 1$ is a prime. Then, by Theorems 9 and 10, number p admits a unique representation (apart from the order of the summands) of the form $p = x^2 + y^2$, where x, y are natural numbers. Obviously, there are no representations of number p other than the sum of two squares of integers because, if there were, one of the squares would be equal to zero, and so p would be the square of a natural number, which is impossible. It is obvious that in the representation $p = x^2 + y^2$ the numbers x, y must be relatively prime; for otherwise, if $(x, y) = d > 1$, we would have $d^2 | p$, which is impossible. We have thus proved that the conditions of the theorem are necessary. In order to show that they are also sufficient, we prove the following.

LEMMA. *If each of two given natural numbers of the form* $4k + 1$ *with* $k > 0$ *is the sum of two squares of integers, then their product does not satisfy the conditions of Theorem* 11.

PROOF OF THE LEMMA. Suppose that $m = a^2+b^2$, $n = c^2+d^2$, where a, b, c, d are integers. We have

$$(28) \qquad mn = (ac+bd)^2+(ad-bc)^2 = (ac-bd)^2+(ad+bc)^2.$$

Suppose that the two decompositions, just obtained, of number mn differ only in the order of summands. Then either $ac+bd = ad+bc$ or $ac+bd = |ac-bd|$. In the first case we have $a(c-d) = b(c-d)$. But $c \neq d$, since otherwise. i.e. when $c = d$, we have $n = 2c^2$, which contradicts the fact that n is an odd number. We then have $a = b$. But this is also impossible, since m is an odd number. In the other case, i.e. when $ac+bd = |ac-bd|$, we have either $ac+bd = ac-bd$ or $ac+bd = bd-ac$. Then in the first of these cases $bd = 0$, and so $b = 0$ or $d = 0$. If $b = 0$, then $m = a^2$, where $a > 1$ and $mn = (ac)^2+(ad)^2$, where ac and ad have a common divisor > 1, consequently number mn does not satisfy the conditions of the theorem. In the second case we have $ac = 0$, and so $a = 0$ or $c = 0$, whence, in analogy to the previous case, we infer that the number mn does not satisfy the conditions of Theorem 11. Thus it only remains to consider the case where decompositions (28) differ.not only in the order of the factors. In this case, however, number mn clearly does not satisfy the conditions of Theorem 11. The lemma is thus proved. ☐

We now return to the proof of the sufficiency of the conditions of Theorem 11. Suppose, to the contrary, that a number $s = 4k+1 > 1$ satisfies the conditions of Theorem 11 and is not a prime. Let p be an arbitrary prime factor of the number s. Clearly p is an odd number. If p were equal to $4t+3$, then, since by assumption $s = a^2+b^2$, where $(a, b) = 1$, we would have $a^2 \equiv -b^2 \pmod{p}$, whence, raising each side of the last congruence to the $\frac{1}{2}(p-1) = (2t+1)$-th power, by Theorem 5, we would obtain $1 \equiv -1 \pmod{p}$, i.e. $2|p$, which is impossible. Thus we see that p must be of the form $4t+1$ and therefore, by Theorem 9, p is the sum of two squares of natural numbers. Hence each prime factor of the number s is the sum of two squares of integers, whence, by (28), each divisor of s has the same property. If the number s could be composite then it would be a product of natural numbers $n, m > 1$, each of them being the sum of two squares of integers and of the form $4t+1$ (since it is the product of prime factors of this form). Therefore, by the lemma, the number $s = mn$ does not satisfy the conditions of Theorem 11, contrary to the assumption. Theorem 11 is thus proved. ☐

Here is an application of Theorem 11. If one has to decide whether a given natural number n of the form $4k+1$ is a prime or not one forms the sequence of numbers.

$$n-0^2, \quad n-1^2, \quad \ldots, \quad n-([\sqrt{n}])^2$$

and checks which of these numbers are squares.

In this way, applying Theorem 11, T. Kulikowski, with the aid of the electronic computer EMC of the Warsaw Polytechnic, has found about 1960 that the number $2^{39}-7$ is a prime because it admits precisely one representation as the sum of two squares of integers,

$$2^{39}-7 = 64045^2+738684^2$$

and the integers are relatively prime.

It is known that the numbers 2^n-7, $n = 4, 5, \ldots, 38$, are composite. The problem whether there exist prime numbers of the form 2^n-7 was formulated by P. Erdős in 1956. We see that the answer is positive.

EXERCISES. 1. Prove that natural numbers $n > 1$ and $n+2$ form a pair of twin primes if and only if the congruence

$$(29) \qquad 4((n-1)!+1)+n \equiv 0 \pmod{n(n+2)}$$

holds (Clement [1], for $n > 3$ already Coblyn [1]).

PROOF. Suppose that the numbers n and $n+2$ are both prime numbers. In view of Theorem 3, we have $(n-1)!+1 \equiv 0 \pmod{n}$ and $(n+1)!+1 \equiv 0 \pmod{n+2}$. But, since $n \equiv -2 \pmod{n+2}$ and $n+1 \equiv -1 \pmod{n+2}$, we see that $(n+1)! \equiv (n-1)!2 \pmod{n+2}$. From this we infer that the left-hand side of (29) is divisible by n and that $4((n-1)!+1)+n \equiv (n+1)!2+2+n+2 = 2((n+1)!+1)+n+2 \equiv 0 \pmod{n+2}$ Therefore the left-hand side of (29) is also divisible by $n+2$. But since the numbers n, $n+2$ are different primes, then the left-hand side of (29) is divisible by the product $n(n+2)$; hence we see that formula (29) holds.

Now, suppose that for a natural number $n > 1$ congruence (29) is valid. If n were even, i.e. if $n = 2k$, where k is a natural number, then we would have $n-1 \leqslant k$, whence $k|(n-1)!$ and $2k|(n-1)!4$. Consequently $(n-1)!4 \equiv 0 \pmod{n}$, which, in view of (29), would imply $4 \equiv 0 \pmod{n}$ and this would give $2k|4$, whence $k|2$ and so $k = 1$ or $k = 2$ and consequently $n = 2$ or $n = 4$. But it is easy to verify that congruence (29) is valid neither for $n = 2$ nor for $n = 4$. Thus we see that congruence (29) implies the congruence $(n-1)!+1 \equiv 0 \pmod{n}$, and this, by Theorem 3^a, shows that n is a prime number. Finally, since, as we have shown above, for natural numbers n the congruence $4((n-1)!+1)+n \equiv 2((n+1)!+1) \pmod{n+2}$ holds, we deduce from (29), using the fact that $n+2$ is odd, that the congruence $(n+1)!+1 \equiv 0 \pmod{n+2}$ is valid. Hence, applying again Theorem 3^a, we conclude that $n+2$ is a prime. We have thus shown that n, $n+2$ is a pair of twin primes. ☐

2. Prove that if $n = a^2+b^2 = c^2+d^2$, where a, b, c, d are natural numbers such that $a \geqslant b$, $c \geqslant d$, $a > c$, $(a, b) = (c, d) = 1$, then the number

$$\delta = \frac{ac+bd}{(ac+bd, ab+cd)} \tag{30}$$

is a divisor of the number n such that $1 < \delta < n$.

PROOF. If $n = a^2+b^2 = c^2+d^2$, then

$$\begin{cases} n^2 = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2, \\ (ac+bd)(ad+bc) = n(ab+cd). \end{cases} \tag{31}$$

Hence $n|(ac+bd)(ad+bc)$. If $n|ac+bd$, then by (31) we have $ad-bc = 0$, whence $a/b = c/d$, which, since $(a, b) = (c, d) = 1$, gives $a = c$, contrary to the assumption that $a > c$. If $n|ad+bc$, then, by (31), $ac-bd = 0$, whence $a/b = d/c$, which, by $(a, b) = (c, d) = 1$, gives $a = d$, contrary to the assumption that $a > c \geqslant d$. Numbers $n_1 = ac+bd$ and $n_2 = ad+bc$ are not divisible by n, which, in view of the relation $n|n_1 n_2$ of Exercise 2, § 6, Chapter I and formula (31) implies that the number δ is a divisor of the number n and $1 < \delta < n$. □

3. Prove the following theorem of Liouville [1]. If p is a prime > 5, then the number $(p-1)!+1$ is not the k-th power of p for any natural number k.

PROOF. As we have proved above, if a natural number n is composite $\neq 4$, then $n|(n-1)!$. Therefore, if p is a prime > 5, then $p-1\,|(p-2)!$, whence $(p-1)^2\,|(p-1)!$. On the other hand, it follows from the binomial formula applied to $(1+(p-1))^k = p^k$, where k is a natural number, that $(p-1)^2\,|1+k(p-1)-p^k$. If $(p-1)!+1 = p^k$, then $(p-1)^2\,|k(p-1)-(p-1)!$ would hold, which, by the formula $(p-1)^2|(p-1)!$, would give $(p-1)^2\,|k(p-1)$, and so $p-1\,|k$, whence $k \geqslant p-1$ and consequently $(p-1)!+1 = p^k \geqslant p^{p-1}$, which is impossible since, of course, $(p-1)! \leqslant (p-1)^{p-2}$. □

4. Prove that if p is a prime > 5, then the number $(p-1)!+1$ has at least two different prime divisors.

PROOF. By Theorem 3, the number $(p-1)!+1$ has at least one prime divisor p. But, since in view of Exercise 3 it is not the k-th power of p for any natural number k, it must have another prime divisor. □

5. Prove the theorem of Lerch [1] stating that if p is an odd prime number, then

$$1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1} \equiv p+(p-1)! \pmod{p^2}.$$

PROOF. Let p be an odd prime number. By Theorem 3 the number $\frac{(p-1)!+1}{p}$ is an integer. Let r be the remainder obtained by dividing it by p; thus we have $\frac{(p-1)!+1}{p} \equiv r \pmod{p}$. Hence $(p-1)! \equiv pr-1 \pmod{p^2}$. In view of Theorem 5, for $a = 1, 2, \ldots, p-1$ the number $\frac{a^{p-1}-1}{p}$ is integral, let r_a be remainder obtained by dividing it by p, thus

$$\frac{a^{p-1}-1}{p} \equiv r_a \pmod{p}.$$

Hence

$$a^{p-1} \equiv pr_a+1 \pmod{p^2}. \tag{32}$$

From this we obtain

$$((p-1)!)^{p-1} = 1^{p-1}\cdot 2^{p-1}...(p-1)^{p-1} \equiv (pr_1+1)(pr_2+1)...(pr_{p-1}+1)$$
$$\equiv 1+p(r_1+r_2+...+r_{p-1})\,(\mathrm{mod}\,p^2).$$

But, since $(p-1)! \equiv pr-1\,(\mathrm{mod}\,p^2)$, we see that

$$((p-1)!)^{p-1} \equiv (pr-1)^{p-1} \equiv 1-(p-1)pr \equiv 1+pr\,(\mathrm{mod}\,p^2).$$

Now, comparing the formulae for $((p-1)!)^{p-1}$, we obtain

$$p(r_1+r_2+ ... +r_{p-1}) \equiv pr\,(\mathrm{mod}\,p^2).$$

whence, by (32),

$$1^{p-1}+2^{p-1}+ ... +(p-1)^{p-1} \equiv p(r_1+r_2+ ... +r_{p-1})+p-1$$
$$\equiv pr+p-1 \equiv (p-1)!+p\,(\mathrm{mod}\,p^2). \quad \square$$

6. Prove that every prime number $p > 5$ is a factor of the number $n_p = 111...1$ written in the scale of ten with the use of $p-1$ digits, each of them equal to 1.

PROOF. Let p be a prime number > 5. Then $(10, p) = 1$ and $9n_p = 10^{p-1}-1$. In view of Theorem 5, $10^{p-1} \equiv 1\,(\mathrm{mod}\,p)$, whence $p\,|\,9n_p$. But, since $(p, 9) = 1$ (for, p is a prime > 5), we must have $p\,|\,n_p$. $\square$

7. Prove that if p is a prime and c an integer, then there exist infinitely many natural numbers x which satisfy each congruence of the following infinite sequence:

$$(*) \qquad x \equiv c\,(\mathrm{mod}\,p), \qquad x^x \equiv c\,(\mathrm{mod}\,p), \qquad x^{x^x} \equiv c\,(\mathrm{mod}\,p), ...$$

PROOF. Let p be a prime and c a given integer. Since $(p, p-1) = 1$, then as is known, there exist infinitely many natural numbers $x > 1$ such that $x \equiv c\,(\mathrm{mod}\,p)$ and $x \equiv 1\,(\mathrm{mod}\,p-1)$. Hence $x^k \equiv 1\,(\mathrm{mod}\,p-1)$ for $k = 1, 2, ...$ Consequently $x^k = 1+(p-1)\,l_k$, where in view of $x > 1$, l_k is a natural number. Hence $x^{x^k} = x\,(x^{l_k})^{p-1}(\mathrm{mod}\,p)$. If $p\,|\,c$, then $x \equiv 0\,(\mathrm{mod}\,p)$ and, clearly, x satisfies each of congruences $(*)$. If c is not divisible by p, then $(c, p) = 1$ and, since $x \equiv c\,(\mathrm{mod}\,p)$, $(x, p) = 1$ and $(x^{l_k}, p) = 1$. Hence, by Theorem 5, we obtain $(x^{l_k})^{p-1} \equiv 1\,(\mathrm{mod}\,p)$ and so $x^{x^k} \equiv x \equiv c\,(\mathrm{mod}\,p)$ for any $k = 1, 2, ...$ Substituting $1, x, x^x, x^{x^x}, ...$ for k successively, we obtain $(*)$. $\square$

Congruences like $(*)$ have been investigated also for arbitrary positive moduli (Schinzel and Sierpiński [4]).

8. Find all the natural numbers each of which admits precisely one representation as the sum of the squares of two relatively prime natural numbers. (Of course we do not consider two representations as being different if they differ only in the order of the summands.)

SOLUTION. We are going to prove that the numbers in question are precisely the powers (the exponents being natural numbers) of the primes of the form $4k+1$.

LEMMA 1. *If p is a prime of the form $4t+1$, then, for $k = 1, 2, ...$, number p^k admits precisely one representation as the sum of the squares of two relatively prime natural numbers.*

PROOF OF LEMMA 1. In virtue of Theorem 11 the lemma is true for $k = 1$. Let k denote an arbitrary natural number and suppose that the lemma is true for number k. Then there exist natural numbers c and d such that $(c, d) = 1$ and $p^k = c^2+d^2$. It follows from Theorem 11 that there exist natural numbers a, b such that $(a, b) = 1$ and such that $p = a^2+b^2$. Hence

$$(33) \qquad p^{k+1} = (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2.$$

If each of the numbers $ad-bc$ and $ac-bd$ is divisible by p, then $ad \equiv bc \pmod p$ and $ac \equiv bd \pmod p$, whence $a^2cd \equiv b^2cd \pmod p$, so $p \mid cd(a^2-b^2)$. But since $p^k = c^2+d^2$ and $(c, d) = 1$, neither of the numbers c and d can be divisible by p. Consequently $p \mid a^2-b^2$, which together with the relation $p \mid a^2+b^2$ gives $p \mid a$ and, since $p = a^2+b^2$, $p \mid b$, contrary to the assumption $(a, b) = 1$. Therefore at least one of the numbers $ad-bc$ and $ac-bd$ is not divisible by p. If this is the number $ad-bc$, then by (33) the number $ac+bd$ is not divisible by p either. Then the numbers $ac+bd$ and $ad-bc$ are relatively prime, since, as follows from (33), each of their common factor is a divisor of p^{k+1} and, as we have just seen, p does not divide any of them. Similarly, if $ac-bd$ is not divisible by p, then the numbers $ad+bc$ and $ac-bd$ are relatively prime. Thus in any case formula (33) gives a representation of p^{k+1} as the sum of the squares of two relatively prime natural numbers. This, by induction, proves that for every $k = 1, 2, \ldots$ the number p^k is the sum of the squares of two relatively prime natural numbers.

We now suppose that for a natural number k the number p^k admits two different representations as the sum of the squares of two relatively prime natural numbers. Let $p^k = a^2+b^2 = c^2+d^2$, where $(a, b) = (c, d) = 1$ and $a \geqslant b$, $c \geqslant d$, $a > c$. We have

$$(34) \qquad p^{2k} = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2,$$

and

$$(ac+bd)(ad+bc) = (ab+cd)p^k.$$

Hence, at least one of the numbers $ac+bd$ and $ad+bc$ is divisible by p. If both were divisible by p, then, by (34), we would have $ad \equiv bc \pmod p$ and $ac \equiv bd \pmod p$, whence $p \mid cd(a^2-b^2)$, and, since $p^k = c^2+d^2$ and $(c, d) = 1$, we would also have $p \mid a^2-b^2$, which, in virtue of $p \mid a^2+b^2$, would give $p \mid 2a^2$, whence, since p is odd, $p \mid a$. But hence, in view of $p \mid a^2+b^2$, we would also obtain $p \mid b$, which contradicts $(a, b) = 1$. Thus precisely one of the numbers $ac+bd$ and $ad+bc$ is divisible by p. But since their product is equal to a multiple of p^k, the one that is divisible by p must be divisible by p^k. If $p^k \mid ac+bd$, then, by (34), $ad-bc = 0$, whence $a/b = c/d$, which, by $(a, b) = (c, d) = 1$, implies $a = c$, contrary to the assumption. If $p^k \mid ad+bc$, then, by (34), $ac-bd = 0$, whence $a/b = d/c$, which, in virtue of $(a, b) = (c, d) = 1$, implies $a = d$, contrary to $a > c \geqslant d$. Lemma 1 is thus proved. □

If follows that in order to prove the theorem if suffices to prove that if an odd natural number admits a unique representation (apart from the possibility of interchanging of the summands) as the sum of the squares of two relatively prime natural numbers, then n is a power with a natural number exponent of a prime of the form $4k+1$.

In order to do this we first prove the following

LEMMA 2. *If m and n are two odd natural numbers which are relatively prime and such that each of them is representable as the sum of the squares of two relatively prime natural numbers, then the product mn admits at least two representations as the sum of the squares of two relatively prime natural numbers which differ not only in the order of the summands.*

PROOF OF LEMMA 2. Suppose that m and n are relatively prime odd natural numbers and

a, b, c, d are natural numbers such that $(a, b) = (c, d) = 1, m = a^2+b^2, n = c^2+d^2$. Suppose that $a \geqslant b$, $c \geqslant d$. We then have

$$mn = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2 \tag{35}$$

and

$$(ac+bd)(ad+bc) = cdm+abn. \tag{36}$$

The decompositions of the number mn into the sum of squares given by (35) are different. The proof follows from the fact that if $ac+bd = ad+bc$, then we would have $(a-b)(c-d) = 0$, and so $a = b$ or $c = d$, which is impossible because the numbers m and n are odd; if $ac+bd = ac-bd$ (number $ac-bd$ is $\geqslant 0$, since $a \geqslant b$, $c \geqslant d$), then we would have $ac = 0$, which is impossible. Thus to complete the proof of Lemma 2 it is sufficient to show that $(ac+bd, ad-bc) = 1$ and $(ad+bc, ac-bd) = 1$. If $(ac+bd, ad-bc) > 1$, then the numbers $ac+bd$ and $ad-bc$ would have a common prime divisor p. Hence, by (35), $p|mn$ and so $p|m$ or $p|n$. If $p|m$, then, by (36), we would have $p|abn$, which, in view of $p|m$ and $(m, n) = 1$, would give $p|ab$, so $p|a$ or $p|b$, which, in virtue of $p|m = a^2+b^2$, would give $p|a$ and $p|b$, contrary to the assumption that $(a, b) = 1$. If $p|n$, then, by (36), $p|cdm$, which, in view of $(m, n) = 1$, would give $p|cd$, which in virtue of $p|c^2+d^2$ and $(c, d) = 1$, leads to a contradiction again. The lemma is thus proved. □

Suppose now that an odd number n has a unique representation as the sum of the squares of two relatively prime natural numbers. Let $n = a^2+b^2$ be this unique representation and let p denote a prime divisor of the number n. Then p is, plainly, an odd number. If $p = 4k+3$, then raising each side of the congruence $a^2 \equiv -b^2 \pmod p$ to the $\frac{1}{2}(p-1) = (2k+1)$-th power we obtain $a^{p-1} \equiv -b^{p-1} \pmod p$, but, in view of the relations $(a, b) = 1$ and $(a, p) = (b, p) = 1$ and Theorem 5 we have $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$. Hence $1 \equiv -1 \pmod p$ that is $p|2$, which is impossible. Thus every prime divisor of number n is of the form $4k+1$. Therefore the factorization of n into primes is of the form $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ and k are natural numbers and each of the primes q_i $(i = 1, 2, \ldots, k)$ is of the form $4t+1$. If $k = 1$, then there is nothing to be proved. Suppose that $k > 1$. Then since any two of the numbers $q_1^{\alpha_1}, q_2^{\alpha_2}, \ldots, q_k^{\alpha_k}$ are relatively prime, Lemma 1 implies that each of them is the sum of the squares of two relatively prime natural numbers. Then Lemma 2 shows that the number $q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_{k-1}^{\alpha_{k-1}}$ is the sum of the squares of two relatively prime numbers and, since $(q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_{k-1}^{\alpha_{k-1}}, q_k^{\alpha_k}) = 1$, the number $q_1^{\alpha_1} \cdot q_2^{\alpha_2} \ldots q_{k-1}^{\alpha_{k-1}} \cdot q_k^{\alpha_k} = n$ has at least two different representations as the sum of the squares of two relatively prime numbers, contrary to the assumption about the number n. Therefore we must have $k = 1$, and this completes the proof (cf. Sierpiński [29]). □

6. Numeri idonei

Under this name we understand numbers d which have the following property: if an odd integer $n > 1$ admits a unique representation (apart from the obvious possibility of interchanging the summands) in the form x^2+y^2d, where x, y are non-negative integers and in this unique representation the summands are relatively prime, then n is a prime (^{1}).

It follows from Theorem 11 that 1 belongs to the class of these numbers. Euler gave the following 65 examples of these numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

Numbers d have been investigated up to $5 \cdot 10^{10}$ (see Weinberger [1]) but no numerus idoneus greater than 1848 has been found.

S. Chowla [1] proved in 1934 that the number of numeri idonei is finite; later he and W. E. Briggs proved that there is at most one square-free greater than 10^{65} (cf. Chowla and Briggs [1]).

Finally P. Weinberger [1] replaced in the last result 10^{65} by 1365. As to numeri idonei which are not square-free they are either less then 100 or of the form $4d$, where d is a numerus idoneus square-free and even. (Grube [1] or Grosswald [1]). More information on numeri idonei is to be found in papers of I. G. Melnikov [1] and J. Steinig [1].

7. Pseudoprime and absolutely pseudoprime numbers

It follows from Theorem 5^a that if n is a prime, then $n | 2^n - 2$. Chinese mathematicians claimed 25 centuries ago that the converse theorem is also true. In fact, this is true for the natural numbers $n \leqslant 300$ (^{2}). Number 341, however, is a composite number, it is equal to the product $11 \cdot 31$, and $341 | 2^{341} - 2$. In fact, since 11 and 31 are odd primes, by Theorem 5 we have $2^{10} \equiv 1 \pmod{11}$ and, clearly, $2^{10} \equiv 1 \pmod{31}$. Hence $2^{341} \equiv 2 \cdot 2^{340} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{31}$. Therefore number $2^{341} - 2$ is divisible by 11 and by 31, and so it is divisible by the product $11 \cdot 31 = 341$.

Composite numbers n for which $n | 2^n - 2$ are called *pseudoprimes*. The pseudoprimes $\leqslant 2000$ are the following: $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$, $1105 = 5 \cdot 13 \cdot 17$, $1387 = 19 \cdot 73$, $1729 = 7 \cdot 13 \cdot 19$,

---

(^{1}) The definitions of these numbers given by many authors are in general incorrect. A correct, though more complicated, definition of the numbers (which he has called *Euler numbers*) has been given by F. Grube [1].

(^{2}) It is worth noticing that in the years 1680–81 Leibniz also claimed that the number $2^n - 2$ is not divisible by n unless n is a prime. His assertion, however, was based on a false argument. (Cf. Dickson [7], Vol. I, p. 64.)

$1905 = 3 \cdot 5 \cdot 127$. P. Poulet [2] has tabulated all the odd pseudoprimes below 10^8 and C. Pomerance, J. L. Selfridge and S. S. Wagstaff Jr. [1] have found them all below $25 \cdot 10^9$.

THEOREM 12. *There are infinitely many pseudoprime numbers* (¹).

LEMMA. *If n is an odd pseudoprime, then the number $m = 2^n - 1$ is also an odd pseudoprime. Clearly $m > n$.*

PROOF OF THE LEMMA. Suppose that n is a pseudoprime. Then n is a composite number and consequently there exists a divisor q of n such that $1 < q < n$. We then have $1 < 2^q - 1 < 2^n - 1 = m$. From this we infer that m is a composite odd number. According to the assumption n is an odd number; therefore, since the fact that n is a pseudoprime implies that $(2^n - 2)/n$ is an integer, we see that number $(2^n - 2)/n$ is an even integer. From this we deduce that $2n | 2^n - 2$, whence $n | 2^{n-1} - 1$. Consequently, for an integer k, we have $2^{n-1} - 1 = kn$. Hence $2^{m-1} = 2^{2^n - 2} = 2^{2kn}$ and so $2^{m-1} - 1 = (2^n)^{2k} - 1$, which implies that $2^n - 1 | 2^{m-1} - 1$ and hence, immediately, $m | 2^m - 2$, i.e. m is a pseudoprime number. It is clear that $m > n$, since, by $n > 2$ (n is a composite number), we have $2^n > n + 1$, and so $m > n$. The lemma is thus proved. □

Theorem 12 is an immediate consequence of the lemma and the fact that there exist odd pseudoprime numbers, for example $n = 341$. □

Denoting by $P(x)$ the number of pseudoprimes less than x we have the following estimates, due to C. Pomerance [3], [4]:

$$\exp(\log x)^{5/14}) < P(x) < x \exp\left(-\frac{\log x \log\log\log x}{2 \log\log x}\right)$$

for sufficiently large x.

Until 1950 only odd pseudoprimes were known. D. H. Lehmer was the first to find an even pseudoprime number. This is $n = 161038$. It was by no means easy to find this number, however, the proof that in fact it is a pseudoprime is quite elementary and simple.

A straightforward verification shows that $n = 2 \cdot 73 \cdot 1103$, $n - 1 = 3^2 \cdot 29 \cdot 617$, $2^9 - 1 = 7 \cdot 73$, $2^{29} - 1 = 233 \cdot 1103 \cdot 2089$. Since $9 | n - 1$ and $29 | n - 1$, we see that $2^9 - 1 | 2^{n-1} - 1$ and $2^{29} - 1 | 2^{n-1} - 1$. From this,

---

(¹) Cf. Cipolla [1], D. H. Lehmer [3], Sierpiński [6].

keeping in mind the relations $73 \mid 2^9 - 1$ and $1103 \mid 2^{29} - 1$, we conclude that the number $2^{n-1} - 1$ is divisible by 73 and 1103. Hence, *a fortiori*, number $2^n - 2$ is divisible by 73 and 1103. But this is an even number, and so it must also be divisible by 2. Hence, looking at the factorization into primes of the number n we see that $n \mid 2^n - 2$. This shows that n is a pseudoprime number.

N. G. W. H. Beeger [1] has proved that there exist infinitely many even pseudoprimes, and later A. Rotkiewicz [2] has proved that the following assertion is also true. *For arbitrary natural numbers a and b there exist infinitely many even numbers n such that $n \mid a^n b - ab^n$.* This in turn, implies that for every natural number a there exist infinitely many even numbers n such that $n \mid a^n - a$(¹). A. Rotkiewicz [5], [6] has proved that there exists infinitely many pseudoprime numbers of the form $ax+b$ $(x = 0, 1, 2, \ldots)$, where a, b are relatively prime integers; $a > 0$ (see also Rotkiewicz [8]).

The pseudoprime numbers are sometimes called *Poulet numbers*, since, as we have already mentioned, Poulet has given the tables of these numbers. The numbers whose every divisor d satisfies the relation $d \mid 2^d - 2$ are called *super-Poulet* numbers (cf. Duparc [2]). An example of a super-Poulet number is the number $n = 2047$. In fact, we have $2047 = 2^{11} - 1 = 23 \cdot 89$, whence, by Theorem 5^a, $11 \mid 2^{11} - 2$, so $2^{11} - 1 \mid 2^{2^{11}-1} - 2$, and this proves that 2047 is a pseudoprime number. The natural factors of 2047 are the numbers 1, 23, 89 and 2047. Hence, since by Theorem 5^a $23 \mid 2^{23} - 2$ and $89 \mid 2^{89} - 2$, we see that 2047 is a super-Poulet number. There exist Poulet numbers which are not super-Poulet. For example, $561 = 3 \cdot 11 \cdot 17$. In fact, the number 560 is divisible by 2, 10 and 16; from this and from Theorem 5 it follows that $3 \mid 2^2 - 1 \mid 2^{560} - 1$, $11 \mid 2^{10} - 1 \mid 2^{560} - 1$, $17 \mid 2^{16} - 1 \mid 2^{560} - 1$. Hence $561 = 3 \cdot 11 \cdot 17 \mid 2^{560} - 1 \mid 2^{561} - 2$, which shows that 561 is a Poulet number. However, number 33, though it is a factor of number 561, is not a divisor of number $2^{33} - 2$; for, $2^{33} - 2$ is not divisible by 11. (In fact, $2^{10} \equiv 1 \pmod{11}$, whence $2^{30} \equiv 1 \pmod{11}$, and so $2^{33} \equiv 8 \pmod{11}$ and $2^{33} - 2 \equiv 6 \pmod{11}$). Thus 561 is not a super-Poulet number.

It follows from Theorem 5^a that a Poulet number which is the product of two different prime factors is a super-Poulet number. Therefore it seems interesting to know whether there exist infinitely many pairs of

---

(¹) Cf. Rotkiewicz [7]. The author proves that for arbitrary natural numbers a, b and every prime number p there exist infinitely many numbers n divisible by p, such that $p \mid a^n b - ab^n$.

different primes p, q such that $pq \mid 2^{pq}-2$. The answer to this question is positive. It follows from the more general theorem of A. Rotkiewicz [1]:

Given three arbitrary natural numbers a, b, s. There exist infinitely many natural numbers n which are the products of s different prime factors and such that $n \mid a^{n-1}-b^{n-1}$.

This theorem implies that for arbitrary natural numbers a and s there exist infinitely many natural numbers n, each of them being the product of s prime factors, such that $n \mid a^n - a$ (for $s = 2$, cf. Schinzel [9], for $a = 2$ see D. H. Lehmer [3], Erdös [8]). This implies, of course, that there exist infinitely many super-Poulet numbers.

On the other hand, it can be proved that there exist infinitely many Poulet numbers which are not super-Poulet (cf. Exercise 1 below).

A composite number n is called an *absolutely pseudoprime number* if for every integer a number $a^n - a$ is divisible by n.

An absolutely pseudoprime number is, *a fortiori*, a pseudoprime, the converse implication, however, not being true.

For example, as we have already seen, number 341 is a pseudoprime, but it is not an absolutely pseudoprime number because number $11^{341}-11$ is not divisible by 31, whence *a fortiori*, it is not divisible by 341. (In fact, we have $11^2 \equiv -3 \pmod{31}$, whence $11^{10} \equiv (-3)^5 \equiv -243 \equiv 5 \pmod{31}$. Therefore $11^{11} \equiv 55 \equiv -7 \pmod{31}$. But, since $11^{30} \equiv 1 \pmod{31}$, $11^{341} \equiv 11^{11} \equiv -7 \pmod{31}$, whence $11^{341}-11 \equiv -18 \pmod{31}$.)

It is easy to prove that if n is the product of k different primes $q_1, q_2, \ldots, q_k$, where k is a natural number > 1, and if $q_i - 1 \mid n-1$, $i = 1, 2, \ldots, k$, then n is an absolutely pseudoprime number. In fact, Theorem 5 proves that, if $i = 1, 2, \ldots, k$ and an integer a is not divisible by q_i, then $q_i \mid a^{q_i-1}-1$. Hence, since $q_i - 1 \mid n-1$, $q_i \mid a^{n-1}-1$ and we have $q_i \mid a^n - a$. The last relation is, of course, true also in the case where $q_i \mid a$.

Hence it follows that number $561 = 3 \cdot 11 \cdot 17$ is an absolutely pseudoprime number; for, number 560 is divisible by 2, 10 and 16. It can be proved that 561 is the least absolutely pseudoprime number.

It is easy to see that for every natural number m if $n = (6m+1)(12m+1)(18m+1)$, number $n-1$ is divisible by $36m$, whence *a fortiori*, it is divisible by $6m$, $12m$ and $18m$. Thus, in consequence of what we have stated above, we see that, *if the numbers $6m+1$, $12m+1$ and $18m+1$ are prime, then $n = (6m+1)(12m+1)(18m+1)$ is an absolutely pseudoprime number* (Chernick [1]).

We do not know whether there exist infinitely many absolutely pseudoprime numbers. Hewever, from Conjecture H (Chapter III, § 8) we infer that there exist infinitely many natural numbers m such that each of the numbers $6m+1$, $12m+1$ and $18m+1$ is a prime. Thus we see that Conjecture H implies the existence of infinitely many absolutely pseudoprime numbers.

The numbers $6m+1$, $12m+1$ and $18m+1$ are primes simultaneously for $m = 1, 6, 35, 45, 51$. This yields the following absolutely pseudoprime numbers: $1729 = 7\cdot 13\cdot 19$, $294409 = 37\cdot 73\cdot 109$, $211\cdot 421\cdot 621$, $271\cdot 541\cdot 811$, $307\cdot 613\cdot 919$.

Here are other absolutely pseudoprime numbers:

$5\cdot 29\cdot 73$, $5\cdot 17\cdot 29\cdot 113$, $5\cdot 17\cdot 29\cdot 113\cdot 337$, $5\cdot 17\cdot 29\cdot 113\cdot 337\cdot 673$,
$5\cdot 17\cdot 29\cdot 113\cdot 337\cdot 673\cdot 2689$, $7\cdot 23\cdot 41$, $7\cdot 31\cdot 73$, $7\cdot 73\cdot 101$,
$7\cdot 13\cdot 31$, $7\cdot 13\cdot 31\cdot 61$, $7\cdot 13\cdot 31\cdot 61\cdot 181$, $7\cdot 13\cdot 31\cdot 61\cdot 181\cdot 541$,
$7\cdot 13\cdot 31\cdot 61\cdot 181\cdot 541\cdot 2161$, $13\cdot 37\cdot 61$, $13\cdot 37\cdot 91$, $13\cdot 37\cdot 241$,
$13\cdot 61\cdot 397$, $13\cdot 97\cdot 421$, $43\cdot 3361\cdot 3907$.

If n is an absolutely pseudoprime number, then, of course, $n|2^n-2$ and $n|3^n-3$. We cannot prove, however, that there exist infinitely many composite numbers for which $n|2^n-2$ and $n|3^n-3$.

If n is an absolutely pseudoprime number and a is an integer relatively prime to n, then, since $a^n-a = a(a^{n-1}-1)$ is divisible by n, number $a^{n-1}-1$ must be divisible by n. Composite numbers n such that $n\,|\,a^{n-1}-1$ holds if $(a, n) = 1$ are called *Carmichael numbers*. Carmichael was the first to notice the existence of these numbers in 1909. We see that any absolutely pseudoprime number is a Carmichael number. It can be proved that the converse is also true. One can prove that a natural number n is a Carmichael number if and only if $n = q_1 q_2 \dots q_k$, where $k \geqslant 3$ and $q_1, q_2, \dots, q_k$ are different odd prime numbers such that $q_i-1\,|\,n-1$, $i = 1, 2, \dots, k$ (cf. Carmichael [2], [3], Sispanov [1], Duparc [1], Knödel [1], Sierpiński [12], pp. 186–188). The best estimate for the number of Carmichael numbers less then a given limit has been given by Pomerance [3].

There are natural numbers $n > 2$ such that for every integer a, $n\,|\,a^{n-2}-a$. For example $n = 195$.

Since $195 = 3\cdot 5\cdot 13$, it is sufficient to prove that for every integer a number $a^{193}-a$ is divisible by 3, 5 and 13. Let p denote any of the numbers 3, 5 or 13. Then, as is easy to verify, $p-1\,|\,192$, because $192 = 4\cdot 48$. If $p|a$, then clearly $p|a^{193}-a$. If p does not divide a, then, by Theorem 5, $p|a^{p-1}-1$, and consequently, since $p-1\,|\,192$, $p|a^{192}-1$, whence $p|a^{193}-a$. Therefore, in either case, the relation $p|a^{193}-a$ holds for any integer a and $p = 3, 5, 13$. Hence $195\,|\,a^{193}-a$ for any integer a.

Similarly, since $399 = 3 \cdot 7 \cdot 19$, $18 \mid 396$, $1023 = 3 \cdot 11 \cdot 31$, $30 \mid 1020$, we can easily prove that for any integer a we have $399 \mid a^{397} - a$, $1023 \mid a^{1021} - a$.

If n is a natural number > 3 such that $n \mid a^{n-2} - a$ for every integer a, then, of course, for $(a, n) = 1$ we have $n \mid a^{n-3} - 1$. Numbers $n > 3$ for which $n \mid a^{n-3} - 1$ holds for $(a, n) = 1$, have been considered by D. C. Morrow [1], who has called them *D numbers*. We prove that *there are infinitely many D numbers*. As a matter of fact, we show that every number of the form $n = 3p$, where p is a prime $\geqslant 3$, is a D number. If $p = 3$, i.e. if $n = 9$, we verify directly that $9 \mid a^6 - 1$ for any a with $(a, 9) = 1$. Suppose that p is a prime > 3, and a is an integer such that $(a, 3p) = 1$. Then, *a fortiori*, $(a, p) = 1$, and so, by Theorem 5, $p \mid a^{p-1} - 1$, whence $p \mid a^{3p-3} - 1$. But, since $(a, 3p) = 1$, the number a is not divisible by 3 and the number $p - 1$ is even (since the number p is an odd prime), therefore $3 \mid a^{3(p-1)} - 1$. This shows that the number $a^{3p-3} - 1$ is divisible by p and by 3; consequently, since $(p, 3) = 1$, it is also divisible by $3p$. Thus we arrive at the conclusion that $3p \mid a^{3p-3} - 1$ holds for any a with $(a, 3p) = 1$, and this means that $3p$ is a D number.

A. Mąkowski [7] has proved a more general theorem, namely that for any natural number $k \geqslant 2$ there exist infinitely many composite numbers n such that for every integer a with $(a, n) = 1$ the relation $n \mid a^{n-k} - 1$ holds. (The proof of this theorem will be given in Chapter VI, § 5.)

EXERCISES. **1.** Prove that there are no even super-Poulet numbers.

PROOF. Suppose, to the contrary, that $2n$ is a super-Poulet number. Then $2n \mid 2^{2n} - 2$, whence $n \mid 2^{2n} - 1$, and this shows that n must be an odd number. Since $2n$ is a super-Poulet number, $n \mid 2^n - 2$, whence, since n is odd, $n \mid 2^{n-1} - 1$. Consequently, since $n \mid 2^{2n-1} - 1$, $n \mid 2^{2n-1} - 2^{n-1} = 2^{n-1}(2^n - 1)$. Hence, using again the fact that n is odd, we obtain $n \mid 2^n - 1$, which, compared with $n \mid 2^n - 2$, proves that $n = 1$, which is impossible, since $2n$ is a composite number. ☐

We have already mentioned Beeger's theorem that there exist infinitely many even Poulet numbers. In view of Exercise 1 these numbers cannot be super-Poulet. Thus we see that there exist infinitely many Poulet numbers which are not super-Poulet.

2. Prove the fact, observed by S. Maciąg, that $n = 2 \cdot 73 \cdot 1103 \cdot 2089$ is a pseudoprime number.

PROOF. We have $n = 2089m$, where, in accordance with what we have proved above, m is a pseudoprime number and $9 \mid m - 1$, $29 \mid m - 1$. Hence $n - 1 = (m - 1)2089 + 2088$. Since $2088 = 2^3 \cdot 3^2 \cdot 29$, by $9 \mid m - 1$ and $29 \mid m - 1$, we infer that $9 \mid n - 1$ and $29 \mid n - 1$. Hence, since $2^9 - 1 = 7 \cdot 73$ and $2^{29} - 1 = 233 \cdot 1103 \cdot 2089$, it follows that $73 \mid 2^{n-1} - 1$, $1103 \mid 2^{n-1} - 1$ and since $2089 \mid 2^{29} - 1$, $2089 \mid 2^{n-1} - 1$. Now, looking at the factorization of number n into prime factors, we see that $n \mid 2^n - 2$. ☐

3. Prove that there exist infinitely many Mersenne numbers which are Poulet numbers.

The proof follows immediately from the lemma in the proof of Theorem 12 and the fact that there exist odd Poulet numbers, for example 341.

However, we do not know whether there exist infinitely many Mersenne numbers which are super-Poulet numbers.

4. Prove that the relation $n \mid 2^n - 1$ cannot hold for a natural number $n > 1$.

PROOF. Suppose to the contrary that n is a natural number greater than 1 such that $n \mid 2^n - 1$ holds. Let p be the least prime divisor of the number n and δ the least natural number for which $p \mid 2^\delta - 1$. Since $p > 1$, we must have $\delta > 1$. Moreover, the relation $p \mid 2^n - 1$ implies $\delta \mid n$. For, if n divided by δ leaves the remainder r with $0 < r < \delta$, then $n = k\delta + r$, whence $2^n - 1 = 2^{k\delta}2^r - 1$. But, since $p \mid 2^\delta - 1$ we have $2^\delta \equiv 1 \pmod{p}$, whence $2^n - 1 \equiv 2^r - 1 \pmod{p}$ and so, since $p \mid 2^n - 1$, we have $p \mid 2^r - 1$, contrary to the definition of δ. In virtue of the theorem of Fermat, $p \mid 2^{p-1} - 1$ (this is because n and, consequently, p are odd). Hence the definition of δ implies that $\delta \leqslant p - 1$ which gives $1 < \delta < p$, contrary to the definition of the prime p.

REMARK. It is easy to prove that there exist infinitely many natural numbers n such that $n \mid 2^n + 1$, for example, such are the numbers $n = 3^k$, where $k = 0, 1, 2, \ldots$ It is also not difficult to prove that there exist infinitely many natural numbers n such that $n \mid 2^n + 2$. In fact, we see that it is trivially true for $n = 2$, and, if n is an even natural number such that $n \mid 2^n + 2$ and $n - 1 \mid 2^n + 1$, then the number $m = 2^n + 2$ satisfies the relations $m \mid 2^m + 2$ and $m - 1 \mid 2^m + 1$. Thus we obtain the numbers $n = 2, 6, 66, \ldots$ It can be proved that there are no natural numbers $n > 1$ such that $n \mid 2^{n-1} + 1$.

5. Prove that there exist infinitely many composite numbers n which satisfy the relation $n \mid a^{n-1} - a$ for any integer a.

HINT. It suffices to put $n = 2p$, where p is an odd prime.

8. Lagrange's theorem

THEOREM 13 (Lagrange). *If n is a natural number and $f(x)$ is a polynomial of degree n with respect to x with integral coefficients; if, moreover, the coefficient of x^n is not divisible by p, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n roots.*

PROOF. It follows from the corollary to Theorem 2 that Theorem 13 is true for $n = 1$. Let n denote an arbitrary natural number > 1 and suppose that Theorem 13 holds for polynomials of degree $n - 1$. Let $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{N-1} x + a_n$ be a polynomial with integral coefficients such that a_0 is not divisible by a prime number p and suppose that the congruence

$$f(x) \equiv 0 \pmod{p} \tag{37}$$

has more than n roots. Then there exist $n+1$ numbers $x_1, x_2, \ldots, x_{n+1}$ which are different roots of congruence (37). Thus, in particular, $f(x_1) \equiv 0 \pmod{p}$. We have

$$f(x)-f(x_1) = a_0(x^n - x_1^n)+a_1(x^{n-1} - x_1^{n-1})+ \ldots +a_{n-1}(x-x_1).$$

But, since

$$x^k - x_1^k = (x-x_1)(x^{k-1}+x^{k-2}x_1 + \ldots + x_1^{k-1}),$$

this gives

$$f(x)-f(x_1) = (x-x_1)g(x), \tag{38}$$

where $g(x)$ is a polynomial of degree $n-1$ with respect to x and integral coefficients. Moreover, the coefficient of x^{n-1} is a_0, which, by assumption, is not divisible by p. Thus, by (38) and the fact that $f(x_1) \equiv 0 \pmod{p}$, congruence (37) is equivalent to the congruence

$$(x-x_1)g(x) \equiv 0 \pmod{p}. \tag{39}$$

Consequently, each of the numbers $x_1, x_2, \ldots, x_{n+1}$ is a root of congruence (39). For $i = 2, 3, \ldots, n+1$ we then have $p \mid (x_i - x_1)g(x_i)$, which, since $x_1, x_2, \ldots, x_{n+1}$ are different roots of congruence (37), implies that $p \mid g(x_i)$ for $i = 2, 3, \ldots, n+1$. This proves that the congruence $g(x) \equiv 0 \pmod{p}$ has at least n different roots, which contradicts the assumption that Theorem 13 holds for polynomials of degree $n-1$.

From this we conclude that congruence (37) cannot have more than n roots, and this, by induction, completes the proof of Theorem 13. □

It is essential for Theorem 13 that the modulus p is prime. For example, the congruence $x^2 - 1 \equiv 0 \pmod{8}$ has four roots: 1, 3, 5, 7; similarly, the congruence $x^2+3x+2 \equiv 0 \pmod{6}$ has four roots 1, 2, 4, 5, though the leading coefficient in either of the congruences is relatively prime to the modulus.

It can be proved that if m is a composite number, then only in the case $m = 4$ the following theorem holds: *if $f(x)$ is a polynomial of degree n with integral coefficients such that the leading coefficient is relatively pime to m, then the congruence $f(x) \equiv 0 \pmod{m}$ has at most n different roots* (cf. Sierpiński [12], pp. 180–181).

COROLLARY. *If a congruence of degree n, with integral coefficients and a prime modulus p has more than n roots, then all the coefficients are divisible by p.*

PROOF. Let (37) be a congruence satisfying the conditions and let

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n.$$

Suppose that among $a_0, a_1, \ldots, a_n$ there are coefficients which are not divisible by p, and let a_m be the first term of the sequence $a_0, a_1, \ldots, a_n$ which is not divisible by p. Then for every integer x we have

$$f(x) \equiv a_m x^{n-m} + a_{m+1} x^{n-m-1} + \ldots + a_{n-1} x + a_n \pmod{p}.$$

If $n = m$, then $f(x) \equiv a_n \pmod{p}$, and, since congruence (37) has more than n roots, there exists an integer x such that $f(x) \equiv 0 \pmod{p}$, whence $a_n \equiv 0 \pmod{p}$. This shows that m must be $< n$. Consequently the polynomial $a_m x^{n-m} + \ldots + = a_{n-1} x + a_n$ satisfies the conditions of Theorem 13, and so it has at most $n - m \leqslant n$ different roots, contrary to the assumption. The corollary is thus proved. ☐

If all the coefficients of a congruence are divisible by the modulus, then, of course, the congruence holds identically. The converse, however, is not true. For example, the congruence $x^2 + x \equiv 0 \pmod{2}$ holds identically. Similarly, by Theorem 5^{a}, the congruence $x^{17} - x \equiv 0 \pmod{17}$ holds identically.

A simple application of Theorem 5^{a} leads us to the conclusion that every congruence, where the modulus is a prime p, is equivalent to a congruence of a degree not greater than p. In fact, by Theorem 5^{α}, for every integer x we have

$$x^p \equiv x \pmod{p}, \qquad x^{p+1} \equiv x^2 \pmod{p}, \qquad \text{and so on.}$$

This shows that any power $\geqslant p$ of the unknown x can be replaced by a power $\leqslant p-1$ of x.

THEOREM 14. *If $m = ab$, where a, b are relatively prime natural numbers, then the number of the roots of the congruence*

$$f(x) \equiv 0 \pmod{m}, \tag{40}$$

where $f(x)$ is a polynomial in x with integral coefficients, is equal to the product of the number of the roots of the congruence

$$f(x) \equiv 0 \pmod{a} \tag{41}$$

and the number of the roots of the congruence

$$f(x) \equiv 0 \pmod{b}. \tag{42}$$

PROOF. If x is a root of congruence (40), then it is a root of each of the congruences (41) and (42). The reason is that, if $m \mid f(x)$, then, *a fortiori*, $a \mid f(x)$ and $b \mid f(x)$. Thus we see that to each root of congruence (40) there corresponds a pair (u, v), u being a root of congruence (41) and v being a root of congruence (42). (To be more precise: u is the remainder obtained by dividing x by a, v is the remainder obtained by dividing x by b.) It is easy to verify that different pairs u, v correspond to different roots of congruence (40). In fact, if to two different roots x, y corresponds the same pair (u, v), then $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b}$, which, in virtue of $(a, b) = 1$, implies $m = ab \mid x-y$ and consequently $x \equiv y \pmod{m}$, contrary to the assumption that the roots x, y are different.

Now suppose that u is a root of congruence (41) and v a root of congruence (42). Then, since $(a, b) = 1$, in virtue of the Chinese remainder theorem (cf. Chapter I, § 12), there exists an integer x such that

$$x \equiv u \pmod{a} \qquad \text{and} \qquad x \equiv v \pmod{b},$$

whence, by Theorem 1, $f(x) \equiv f(u) \pmod{a}$ and $f(x) \equiv f(v) \pmod{b}$. But, since $f(u) \equiv 0 \pmod{a}$ and $f(v) \equiv 0 \pmod{b}$, we have $f(x) \equiv 0 \pmod{a}$ and $f(x) \equiv 0 \pmod{b}$; consequently, since $(a, b) = 1$ and $ab = m$, $f(x) \equiv 0 \pmod{m}$.

Thus we have shown that to each pair (u, v) where u is a root of congruence (41) and v is a root of congruence (42), there corresponds a root of congruence (40). This proves the existence of a one-to-one correspondence between all the roots (non-congruent with respect to the modulus m) of congruence (40) and all the pairs (u, v) consisting of the roots of congruences (41) and (42), respectively. Thus we see that the number of the roots of congruence (40) is equal to the number of the pairs (u, v) where u is a root of congruence (41) and v is a root of congruence (42). Hence Theorem 14 follows. □

COROLLARY. *If $m = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ is the factorization of an integer m into primes, then the number of the roots of congruence* (40) *is equal to the product of the numbers of the roots of the following k congruences:*

$$f(x) \equiv 0 \pmod{q_1^{\alpha_1}}, \quad f(x) \equiv 0 \pmod{q_2^{\alpha_2}}, \quad \ldots, \quad f(x) \equiv 0 \pmod{q_k^{\alpha_k}}.$$

This gives a method of reducing the solution of a congruence with respect to an arbitrary modulus m to the solution of congruences with respect to moduli each of which is a power of a prime number.

EXERCISE. Prove that for every natural number n there exists a modulus m such that the congruence $x^2 \equiv 1 \pmod{m}$ has more than n roots.

PROOF. If p is an odd prime, then the congruence $x^2 \equiv 1 \pmod{p}$ has precisely two roots, 1 and $p-1$ (cf. § 5). It follows from the corollary to Theorem 14 that the congruence $x^2 \equiv 1 \pmod{p_2 p_3 \dots p_{s+1}}$ has precisely 2^s roots. Thus it remains to find a natural number s such that $2^s > n$. For example, the congruence $x^2 \equiv 1 \pmod{105}$ has 8 roots, since $105 = p_2 p_3 p_4$. (The roots are 1, 29, 34, 41, 64, 71, 76, 104.) □

9. Congruences of the second degree

Let us consider a congruence of the second degree

$$ax^2+bx+c \equiv 0 \pmod{m}, \tag{43}$$

where m is a given natural number, and a, b, c are given integers. We assume that $a \not\equiv 0 \pmod{m}$, since otherwise if $a \equiv 0 \pmod{m}$, (43) becomes a congruence of degree less than two.

Since the relation $m \mid ax^2+bx+c$ is equivalent to the relation $4am \mid 4a(ax^2+bx+c)$, congruence (43) is equivalent to the congruence

$$4a(ax^2+bx+c) \equiv 0 \pmod{4am}. \tag{44}$$

Let $D = b^2-4ac$. Then, in virtue of the identity

$$4a(ax^2+bc+c) = (2ax+b)^2-(b^2-4ac),$$

congruence (44) can be rewritten in the form

$$(2ax+b)^2 \equiv D \pmod{4am}. \tag{45}$$

Let x be a root of congruence (43) and let $z = 2ax+b$. Then, by (45), z is a root of the binomial congruence

$$z^2 \equiv D \pmod{4am}. \tag{46}$$

Thus, we see that to each root x of congruences (43) corresponds a root of congruence (46).

In order to establish the converse correspondence, that is, to find for a given root z of congruence (46) all the roots x of (43) to which the root z corresponds, we have to solve the congruence $2ax+b \equiv z \pmod{4am}$. (This, as we know, is solvable whenever $(2a, 4am) \mid z-b$, i.e. whenever $2a \mid z-b$.) Thus we arrive at the conclusion that the solution of a congruence of the second degree can be reduced to the solution of a congruence of the first degree and a binomial congruence (46). In view of the remark in the corollary to Theorem 14, solution of congruence (46) reduces to the solution of the congruences

$$z^2 \equiv D \pmod{p^\alpha}, \tag{47}$$

where p is a prime and α is a natural number.

We are going to solve congruence (47) now. At first we suppose that $p \mid D$. Then $D = p^\mu D_1$, where μ is a natural number and D_1 is not divisible by p.

If $\mu \geqslant \alpha$, then $D \equiv 0 \pmod{p^\alpha}$ and so (47) becomes the congruence $z^2 \equiv 0 \pmod{p^\alpha}$, which is easy to solve.

If $\mu < \alpha$, the congruence (47) is equivalent to the equation

$$z^2 = p^\mu(D_1 + tp^{\alpha-\mu}), \tag{48}$$

where t is a suitably chosen integer and the number $D_1 + tp^{\alpha-\mu}$ is not divisible by p (because D_1 is not divisible by p). Hence we infer that μ is the highest exponent of p for which p^μ divides z^2. Consequently, μ must be an even number. We then write $\mu = 2\lambda$, where λ is a natural number. Hence $z = p^\lambda z_1$ and so, by (48), $z_1^2 = D_1 + tp^{\alpha-\mu}$. This yields the congruence

$$z_1^2 \equiv D_1 \pmod{p^{\alpha-\mu}}.$$

Thus we see that the solution of congruence (47) reduces to the solution of a congruence of the same type, the right-hand side of which is not divisible by p. We then suppose in congruence (47) that $D \not\equiv 0 \pmod{p}$. If z satisfies this congruence, then, *a fortiori*, it satisfies the congruence

$$z^2 \equiv D \pmod{p},$$

which proves that D is a quadratic residue for the modulus p. From this we conclude that a necessary condition for the solvability of congruence (47) (with D not divisible by p) is that D should be a quadratic residue for the modulus p. We prove that this condition is also sufficient. For this purpose, it is of course sufficient to prove that, if the congruence

$$z^2 \equiv D \pmod{p^{\alpha-1}}, \tag{49}$$

where α is a natural number > 1, is solvable, then congruence (47) is solvable as well.

The cases where p is odd and $p = 2$ are treated separately.

At first we suppose that p is odd. Let y be an integer satisfying congruence (49). Then

$$y^2 \equiv D \pmod{p^{\alpha-1}}. \tag{50}$$

Hence it follows that the number

$$M = \frac{y^2 - D}{p^{\alpha-1}} \tag{51}$$

is an integer. Denote by x the root of the congruence

$$2xy + M \equiv 0 \pmod{p}. \tag{52}$$

The solvability of (52) follows from the fact that since D is not divisible by p, y is not divisible by p, whence, since p is odd, $2y$ is not divisible by p. Let $z = y + p^{\alpha-1}x$. Hence $z^2 = y^2 + 2p^{\alpha-1}xy + p^{2\alpha-2}x^2$. Since, by (51), $y^2 = D + Mp^{\alpha-1}$, we see that

$$z^2 = D + (2xy + M)\,p^{\alpha-1} + x^2p^{2\alpha-2} \tag{53}$$

holds. In view of (52), number $2xy + M$ is divisible by p. In virtue of $2\alpha - 2 = \alpha + (\alpha - 2) \geqslant \alpha$ (since $\alpha > 1$), $p^\alpha \mid p^{2\alpha-2}$. Therefore, by (53), z satisfies congruence (47). Thus we have shown that the condition is sufficient. We formulate the result as follows:

THEOREM 15. *Congruence* (47), *where p is an odd prime, α a natural number and D an integer not divisible by p, is solvable if and only if D is a quadratic residue for the modulus p.*

We now prove that under the conditions of Theorem 15 congruence (47) has precisely two roots.

If z is a root of congruence (47), then, clearly, the number $z_1 = -z$ is also a root of that congruence. Moreover, z and z_1 are not congruent with respect to the modulus p^α, since, if they were, we would have $p^\alpha \mid 2z$, which, since p is odd, would give $p^\alpha \mid z$ and hence $p \mid D$, contrary to the assumption. Thus we see that there exist at least two different roots of congruence (47): z and z_1. We are going to prove that they are the only roots of (47). Suppose that t is a root of congruence (47). Then $t^2 \equiv D \pmod{p^\alpha}$, which by $z^2 \equiv D \pmod{p^\alpha}$ implies $t^2 \equiv z^2 \pmod{p^\alpha}$. Hence $p^\alpha \mid (t-z)(t+z)$. If the numbers $t-z$ and $t+z$ were both divisible by p, then $p \mid 2z$, which since p is odd, would give $p \mid z$ and hence $p \mid D$, contrary to the assumption. Consequently, one of the numbers $t-z$ and $t+z$ is not divisible by p. If $t+z$ is not divisible by p, then $p^\alpha \mid t-z$, that is, $t \equiv z \pmod{p^\alpha}$, if $t-z$ is not divisible by p, then $p^\alpha \mid t+z$, whence $t \equiv -z \pmod{p^\alpha}$. Thus we see that each root of congruence (47) is congruent with respect to the modulus p^α either to z or to $-z$. This proves that congruence (47) has precisely two roots.

Now, let $p = 2$. Then for $\alpha = 1$ formula (47) gives $z^2 \equiv D \pmod 2$, where D which is not divisible by 2, is odd. An immediate consequence of this is that in this case the congruence has precisely one solution, namely $z = 1$.

For $\alpha = 2$ the congruence has the form $z^2 \equiv D \pmod 4$. But the square of an integer is congruent with respect to the modulus 4 either to zero or to 1. Hence, since D is odd, the congruence is solvable only in the case where D is of the form $4k+1$. Then, as can be verified directly, the congruence has two solutions, $z = 1$ and $z = 3$.

For $\alpha = 3$ the congruence is of the form $z^2 \equiv D \pmod 8$. Since D is odd, number z must also be odd, whence, since the square of an odd integer is $\equiv 1 \pmod 8$, we see that for the congruence to be solvable it is necessary that D should be of the form $8k+1$.As is easy to verify, the condition is also sufficient and the congruence has four solutions: 1, 3, 5, 7.

Now let $\alpha > 3$. We have to consider the congruence

$$z^2 \equiv D \pmod{2^\alpha} \qquad \text{where} \qquad \alpha > 3. \tag{54}$$

We see that congruence (54) implies the congruence $z^2 \equiv D \pmod 8$. For the latter to be solvable it is necessary that $D = 8k+1$. We prove that this, in turn, is a sufficient condition for the solvability of (54). To do this suppose that $D = 8k+1$ and that the congruence

$$z^2 \equiv D \pmod{2^{\alpha-1}} \tag{55}$$

is solvable. (This, as proved above, is true for $\alpha = 4$.) Then there exists an integer y such that $y^2 \equiv D \pmod{2^{\alpha-1}}$ and, since D is odd, y, of course, must also be odd. Let

$$M = \frac{y^2 - D}{2^{\alpha-1}}. \tag{56}$$

Then M is an integer. Further, let x be the root of the congruence

$$xy + M \equiv 0 \pmod 2, \tag{57}$$

of the first degree with respect to x. This is solvable since the coefficient y of the unknown and modulus 2 are relatively prime. Let $z = y + x2^{\alpha-2}$. In virtue of (56) we have

$$z^2 = y^2 + xy2^{\alpha-1} + x^2 2^{2\alpha-4} = D + (xy+M)\,2^{\alpha-1} + x^2 2^{2\alpha-4}. \tag{58}$$

But, in view of (57), the number $xy+M$ is even, whence $(xy+M)\,2^{\alpha-1} \equiv 0 \pmod{2^\alpha}$ and, in virtue of $2\alpha-4 = \alpha+(\alpha-4) \geqslant \alpha$ (which is valid because $\alpha \geqslant 4$), $x^2 2^{2\alpha-4}$ is divisible by 2^α: Consequently, $x^2 2^{2\alpha-4}$

$\equiv 0 \pmod{2^\alpha}$. Thus we see that (58) implies (54), which proves that for any $\alpha > 3$ the solvability of congruence (55) implies the solvability of congruence (54). But since, as we have assumed, $D = 8k+1$, congruence $z^2 \equiv D \pmod{2^3}$ is solvable; hence, by induction we see that (for $D = 8k+1$) congruence (54) is solvable for the natural numbers $\alpha \geqslant 3$. We have thus proved the following

THEOREM 16. *In order that the congruence* $z^2 \equiv D \pmod{2^\alpha}$, *where* D *is odd and* α *is a natural number, be solvable, it is necessary and sufficient that* D *should be of the form* $2k+1$, $4k+1$ *or* $8k+1$ *depending on whether* $\alpha = 1$, $\alpha = 2$ *or* $\alpha > 2$.

We now prove that for $\alpha \geqslant 3$ congruence (54) (with $D = 8k+1$) has precisely four roots.

We have proved that (under the assumptions made) the congruence has at least one root. Denote it by z_0. Let z be an arbitrary root of congruence (54). We have $z_0^2 \equiv D \pmod{2^\alpha}$, whence, by (54), $2^\alpha \mid (z-z_0)(z+z_0)$. Since D is odd, the numbers z and z_0 are also odd, whence it follows that the numbers $z-z_0$ and $z+z_0$ are even. They cannot both be divisible by 4, since if they were, number $2z$ would be divisible by 4, and so $2 \mid z$, which is impossible. Thus one of the numbers $z-z_0$, $z+z_0$ is not divisible by 4. If $z-z_0$ is not divisible by 4, then number $\frac{1}{2}(z-z_0)$ is odd. But, since $2^{\alpha-1} \mid \frac{1}{2}(z-z_0)(z+z_0)$, we have $2^{\alpha-1} \mid z+z_0$, and consequently $z = -z_0 + 2^{\alpha-1}t$, where t is an integer. If t is even, then $z = -z_0 \pmod{2^\alpha}$; if t is odd, then $z = -z_0 + 2^{\alpha-1} \pmod{2^\alpha}$. Now we consider the other case, i.e., that $z+z_0$ is not divisible by 4. Then the number $\frac{1}{2}(z+z_0)$ is odd, whence, in virtue of $2^{\alpha-1} \mid (z-z_0)\frac{1}{2}(z+z_0)$, we infer that $2^{\alpha-1} \mid z-z_0$, and so $z = z_0 + 2^{\alpha-1}u$, where u is an integer. If u is even, this gives $z \equiv z_0 \pmod{2^\alpha}$; if u is odd, then $z = z_0 + 2^{\alpha-1} \pmod{2^\alpha}$.

We have thus proved that any root z of congruence (54) must satisfy one of the following four congruences:

$$z \equiv -z_0 \pmod{2^\alpha}, \qquad z \equiv -z_0 + 2^{\alpha-1} \pmod{2^\alpha},$$
$$z \equiv z_0 \pmod{2^\alpha}, \qquad z \equiv z_0 + 2^{\alpha-1} \pmod{2^\alpha}. \tag{59}$$

This shows that the number of the roots cannot be greater than four. On the other hand, it is easy to verify that each number given by any of the congruences (59) satisfies congruence (54) (whenever it is true for z_0) and, since for $\alpha \geqslant 3$ any two of these numbers are not congruent with respect to the modulus 2^α, we see that they are different roots of congruence (54).

The results we have obtained can be formulated in the following

THEOREM 17. *In order that the congruence* $z^2 \equiv D \pmod{m}$, *where* D *is an integer and* $(D, m) = 1$, *be solvable it is necessary and sufficient that* (i) D *should be a quadratic residue for every modulus that is an odd prime factor of number* m *and* (ii) D *should be of the form* $4k+1$ *for* m *divisible by* 4 *but not divisible by* 8 *and of the form* $8k+1$ *for* m *divisible by* 8. *The number of the roots of the congruence is equal to* $2^{\lambda+\mu}$, *where* λ *is the number of odd prime factors of the number* m *and* $\mu = 0$ *for* m *not divisible by* 4, $\mu = 1$ *for* m *divisible by* 4 *but not divisible by* 8, *and, finally,* $\mu = 2$ *for* m *divisible by* 8.

CHAPTER VI

EULER'S TOTIENT FUNCTION AND THE THEOREM OF EULER

1. Euler's totient function

The number of natural numbers $\leqslant n$ that are relatively prime to n is denoted by $\varphi(n)$ (n being a natural number). The function $\varphi(n)$ thus obtained is called *Euler's totient function.* In fact, Euler was the first to investigate this function and its properties in the year 1760. The notation $\varphi(n)$, however, is due to Gauss (it was introduced by him in 1801) — this is the reason why some authors call the function $\varphi(n)$ *Gauss's function.*

It follows immediately from the definition of $\varphi(n)$ that $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$.

If n is a prime, then, of course, every natural number less than n is relatively prime to n; accordingly for prime n,

$$\varphi(n) = n-1. \tag{1}$$

If, however, a natural number n is composite, i.e. has a divisor d such that $1 < d < n$, then in the set $1, 2, \ldots, n$ there are at least the two numbers, n and d, that are not relatively prime to n; therefore $\varphi(n) \leqslant n-2$. Finally, for $n = 1$ we have $\varphi(n) = n > n-1$. We thus see that formula (1) holds only in the case where n is a prime.

This establishes the truth of the following theorem:

A natural number $n > 1$ is a prime if and only if for every natural number $a < n$ the congruence $a^{n-1} \equiv 1 \pmod n$ holds.

In fact, the congruence implies that $(a, n) = 1$, and so, if it is valid for any $a < n$, then $\varphi(n) = n-1$, and consequently n is a prime. The condition is thus sufficient. Its necessity follows immediately from the theorem of Fermat (Theorem 5, Chapter V).

It is easy to evaluate $\varphi(n)$ for any prime power $n = p^k$, k being a natural number.

The only numbers in the set $1, 2, \ldots, p^k$ which are not relatively prime to p^k are those that are divisible by p. These are the numbers pt, where t is a natural number such that $pt \leqslant p^k$, that is, such that $t \leqslant p^{k-1}$. Clearly the number of the t's is p^{k-1}. Hence it follows that in the sequence $1, 2, \ldots, p^k$ there are exactly p^{k-1} numbers which are not relatively prime to p^k; consequently, $\varphi(p^k) = p^k - p^{k-1}$. We have thus proved

THEOREM 1. *If p is a prime and k a natural number, then*

$$\varphi(p^k) = p^{k-1}(p-1).$$

In order to obtain a formula for $\varphi(n)$, where n is an arbitrary natural number, we prove the following

LEMMA. *Let m be a natural number, l a natural number relatively prime to m, and r an arbitrary integer. Then, dividing the numbers*

$$r,\ l+r,\ 2l+r, \ldots, (m-1)\,l+r \tag{2}$$

by m, we obtain the set of remainders

$$0, 1, 2 \ldots, m-1. \tag{3}$$

PROOF. Suppose that for some integers k and h with $0 \leqslant k < h < m$ the numbers $kl+r$ and $hl+r$ yield the same remainder when divided by m. Then the difference between these numbers, equal to $(h-k)\,l$, is divisible by m, whence, in view of $(l, m) = 1$, $m \mid h-k$, which is impossible since $0 < h-k < m$. Thus we see that dividing numbers (2) by m we obtain different remainders. But the number of numbers (2) is m, and this is equal to the number of the residues mod m, i.e. to the number of numbers (3). The lemma is thus proved. □

THEOREM 2. *If l and m are relatively prime natural numbers, then*

$$\varphi(lm) = \varphi(l)\,\varphi(m). \tag{4}$$

PROOF. Since $\varphi(1) = 1$, theorem 2 is valid if at least one of the numbers l, m is equal to 1. Suppose that $l > 1$ and $m > 1$. As we know, number $\varphi(lm)$ is equal to the number of all the terms of the table

$$\begin{array}{cccccc}
1, & 2, & \ldots, & r, & \ldots, & l \\
l+1, & l+2, & \ldots, & l+r, & \ldots, & 2l \\
2l+1, & 2l+2, & \ldots, & 2l+r, & \ldots, & 3l \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
(m-1)\,l+1, & (m-1)\,l+2, & \ldots, & (m-1)\,l+r, & \ldots, & ml
\end{array}$$

that are relatively prime to lm, i.e. to the number of terms which are relatively prime both to l and to m.

Let r be a given natural number $\leqslant l$. We consider the rth column of the table. If $(r, l) = 1$, then all the numbers of the column are relatively prime to l; if $(r, l) > 1$, none of the numbers of the column is relatively prime to l. The number of the natural numbers $r < l$ for which $(r, l) = 1$ is of course $\varphi(l)$, this being the number of the columns in which all the numbers are relatively prime to l. Let us consider one of these columns, say the rth. According to the lemma, the remainders obtained by dividing the numbers of the column by m fill up the set $0, 1, 2, \ldots, m-1$, whence the number of the numbers of the column, which are relatively prime to m, is $\varphi(m)$. This shows that in each of the $\varphi(l)$ columns, the terms of which are relatively prime to l, there are $\varphi(m)$ numbers relatively prime to m. Therefore the total number of the numbers of the table, which are relatively prime to m and to l, is $\varphi(l)\varphi(m)$. This completes the proof of the theorem. □

From Theorem 2, by an easy induction, we obtain the following

COROLLARY. *If* $m_1, m_2, \ldots, m_k$ *are natural numbers any two of which are relatively prime, then*

$$\varphi(m_1 m_2 \ldots m_k) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_k).$$

Now let n be a natural number > 1 and $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ its factorization into prime factors. Applying the formula, just proved, for $m_i = q_i^{\alpha_i}$, $i = 1, 2, \ldots, k$, we obtain the formula

$$\varphi(n) = \varphi(q_1^{\alpha_1})\varphi(q_2^{\alpha_2})\ldots\varphi(q_k^{\alpha_k}).$$

But since, by Theorem 1, $\varphi(q_i^{\alpha_i}) = q_i^{\alpha_i - 1}(q_i - 1)$ holds for $i = 1, 2, \ldots, k$, the following theorem is valid:

THEOREM 3. *If a natural number* $n > 1$ *yields the factorization into prime factors* $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$, *then*

$$\varphi(n) = q_1^{\alpha_1 - 1}(q_1 - 1)\, q_2^{\alpha_2 - 1}(q_2 - 1) \ldots q_k^{\alpha_k - 1}(q_k - 1). \tag{5}$$

This can be rewritten in the form

$$\varphi(n) = n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_k}\right). \tag{6}$$

From Theorem 3 one can easily deduce that, if $(a, b) \neq 1$, then $\varphi(ab) > \varphi(a)\varphi(b)$ and that, if $m \mid n$, then $\varphi(m) \mid \varphi(n)$.

THEOREM 4. *We have*

$$\lim_{n\to\infty} \varphi(n) = +\infty.$$

PROOF (due to J. Browkin). It is sufficient to show that the inequality $\varphi(n) \geqslant \frac{1}{2}\sqrt{n}$ holds for any natural number n. Clearly, the inequality is valid for $n = 1$. Suppose that $n > 1$ and let $n = 2^{\alpha_0} q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ be the factorization of number n into prime factors, α_0 being a non-negative integer and $\alpha_1, \alpha_2, \ldots, \alpha_k$ natural numbers. For an arbitrary natural number $a > 2$ we have $a - 1 > \sqrt{a}$, and for any natural number b the inequality $b - \frac{1}{2} \geqslant \frac{1}{2}b$ holds. Hence, by Theorem 3,

$$\begin{aligned}\varphi(n) &\geqslant 2^{\alpha_0-1} q_1^{\alpha_1-1} q_2^{\alpha_2-1} \ldots q_k^{\alpha_k-1}(q_1-1)(q_2-1)\ldots(q_k-1)\\ &\geqslant 2^{\alpha_0-1} q_1^{\alpha_1-\frac{1}{2}} q_2^{\alpha_2-\frac{1}{2}} \ldots q_k^{\alpha_k-\frac{1}{2}} \geqslant 2^{\alpha_0-1} q_1^{\frac{1}{2}\alpha_1} q_2^{\frac{1}{2}\alpha_2} \ldots q_k^{\frac{1}{2}\alpha_k}\\ &\geqslant \tfrac{1}{2}\sqrt{n}. \quad \square\end{aligned}$$

In connection with Theorem 4 we note that there exist infinitely many natural numbers n such that $\varphi(n) > \varphi(n+1)$.

In order to show this we prove

THEOREM 5. *If n is a composite natural number, then*

$$\varphi(n) \leqslant n - \sqrt{n}. \tag{7}$$

PROOF. Let n denote a composite number and p_1 the least prime divisor of it. As we know, $p_1 \leqslant \sqrt{n}$, so, by formula (6),

$$\varphi(n) \leqslant n\left(1 - \frac{1}{p_1}\right) \leqslant n - \frac{n}{\sqrt{n}},$$

which proves inequality (7). $\square$

Now suppose that *n is a prime number* > 7. Then $n+1$ is a composite number and $n+1 \geqslant 9$. Hence $\sqrt{n+1} \geqslant 3$ and, by (7), $\varphi(n+1) \leqslant n+1 - \sqrt{n+1} \leqslant n-2$. But, since $\varphi(n) = n-1$, we have $\varphi(n) > \varphi(n+1)$. We see that this inequality is valid for any prime number $n > 7$ (as is easy to prove, it holds for $n = 5$ and also for $n = 7$); consequently, it holds for infinitely many natural numbers n.

The equation $\varphi(n) = \varphi(n+1)$ in natural numbers n has been a subject of interest for several authors (cf. Klee [2], Moser [1], Lal and Gillard [1], Yorinaga [1], Baillie [1], [2]).

As has been verified, all the solutions of the equation in natural numbers $n \leqslant 10000$ are the numbers $n = 1, 3, 15, 104, 164, 194, 255, 495, 584, 975, 2204, 2625, 2834, 3255, 3705, 5186, 5187$. It follows that the least natural number n which satisfies the equation $\varphi(n) = \varphi(n+1) = \varphi(n+2)$ is the number 5186. (It is easy to verify that the number 5186 indeed satisfies the equation. This follows immediately from the factorization of the following numbers into prime factors: $5186 = 2 \cdot 2593$, $5187 = 3 \cdot 7 \cdot 13 \cdot 19$, $5188 = 2^2 \cdot 1297$ and from $2592 = 2 \cdot 6 \cdot 12 \cdot 18 = 2 \cdot 1296$.)

We do not know whether there exist infinitely many natural numbers n for which $\varphi(n) = \varphi(n+1)$. For $n \leqslant 2 \cdot 10^8$ there are 391 of them, but none except $n = 5186$ satisfies $\varphi(n) = \varphi(n+1) = \varphi(n+2)$. As regards the equation $\varphi(n+2) = \varphi(n)$, we know that for $n \leqslant 4 \cdot 10^6$ it has 7998 solutions (for $n \leqslant 100$ these are $n = 4, 7, 8, 10, 26, 32, 70, 74$). The equation $\varphi(n+3) = \varphi(n)$, however, has only two solutions, $n = 3$ and $n = 5$, for $n \leqslant 10^6$.

It is easy to prove that for any given natural number k the equation $\varphi(n+k) = \varphi(n)$ has at least one solution in natural numbers n (cf. Exercise 11 below). It follows from the Conjecture H (cf. Chapter III, § 8) that it has infinitely many solutions for any even natural number k (cf. Schinzel and Sierpiński [3], p. 195). A. Schinzel and Andrzej Wakulicz [1] have proved that for every natural number $k \leqslant 2 \cdot 10^{58}$ the equation $\varphi(n+k) = \varphi(n)$ has at least two solutions in natural numbers n (cf. also Schinzel [8]).

If each of the numbers n and $n+2$ is prime, then $\varphi(n+2) = \varphi(n)+2$. The equation, however, is satisfied also by composite numbers, for example $n = 12, 14, 20, 44$. Moser [1] has proved that there are no composite odd numbers $n < 10000$ that satisfy this equation. This suggests a conjecture that there are no odd numbers n, except for the pairs of twin primes $n, n+2$ for which the equality $\varphi(n+2) = \varphi(n)+2$ holds. In this connection A. Mąkowski [4] has raised the question whether there exist composite natural numbers n for which the equalities $\varphi(n+2) = \varphi(n)+2$ and $\sigma(n+2) = \sigma(n)+2$ hold simultaneously.

If n is a prime, then $\varphi(n) = n-1$, so $\varphi(n) | n-1$. We do not know whether there exist composite natural numbers n for which $\varphi(n)|$

$| n-1$ (¹). On the other hand, it is easy to find all the natural numbers n for which $\varphi(n) | n$. It has been proved that all the numbers with this property are the numbers $n = 2^\alpha$, $\alpha = 0, 1, 2, \ldots$, and $n = 2^\alpha 3^\beta$, where α, β, are natural numbers (cf. Sierpiński [26], pp. 196-197).

It follows from (5) that if $n = 2^\alpha$, where α is a natural number > 1, then $\varphi(n) = 2^{\alpha-1}$. Consequently, $2 | \varphi(2^\alpha)$ for $\alpha = 2, 3, \ldots$ If, however, n has an odd prime divisor p, then the number $p-1$ is even and therefore, by (5), $p-1 | \varphi(n)$ and so $2 | \varphi(n)$. Since any natural number > 2 either is the kth power of 2 with $k > 1$ or has an odd prime divisor, we see that for any natural number $n > 2$ the relation $2 | \varphi(n)$ holds.

Since $\varphi(1) = \varphi(2) = 1$, the equation $\varphi(x) = m$, m being odd, is solvable only in the case where $m = 1$. Thus it is shown that there exist infinitely many (odd) natural numbers m for which the equation $\varphi(x) = m$ is unsolvable in natural numbers x. On the other hand, it can be proved that there exist infinitely many even natural numbers m for which the equation $\varphi(x) = m$ has no solutions in natural numbers x. We show this by proving that this is the case for the numbers $m = 2 \cdot 5^{2k}$, where $k = 1, 2, \ldots$, for instance. It follows from (5) that if $\varphi(n) = 2 \cdot 5^{2k}$, where k is a natural number, then n must have precisely one odd prime divisor. The argument is that if q_1 and q_2 were two different odd prime divisors of the number n, then by (5), $(q_1-1)(q_2-1) | \varphi(n) = 2 \cdot 5^{2k}$ and so $4 | \varphi(n)$, which is impossible. Therefore we must have $n = 2^\alpha p^\beta$, where α is an integer $\geqslant 0$ and β a natural number. Moreover, $\alpha \leqslant 1$, since otherwise, if $\alpha \geqslant 2$, $2^{\alpha-1}(p-1) | \varphi(n)$, and so $4 | \varphi(n)$, which is impossible. In the case of $\alpha = 0$, we have $n = p^\beta$ and, in the case of $\alpha = 1$, $n = 2p^\beta$; so in either case we have $\varphi(n) = p^{\beta-1}(p-1) = 2 \cdot 5^{2k}$. If β were > 1, then $p = 5$ and so $p-1 = 4$, which is impossible. Therefore $\beta = 1$, whence $p = 2 \cdot 5^{2k}+1$ which is impossible since the number $5^{2k} = (5^k)^2$ is congruent to 1 with respect to the modulus 3, whence $3 | p$, so $p = 3$ and this is clearly false. Thus we see that the equation $\varphi(n) = 2 \cdot 5^{2k}$, where $k = 1, 2, \ldots$, has no solutions in natural numbers.

By a similar method a stronger theorem has been proved by A. Schinzel [6]. The theorem states that for every natural number s there exists a natural number m divisible by s and such that the equation $\varphi(n) = m$ has no solutions in natural numbers n. This theorem in turn is an

---

(¹) D.H. Lehmer [1] has conjectured that there are no such numbers; G.L. Cohen and P. Hagis Jr. [1] have proved that if they exist, they must have at least fourteen prime factors.

immediate consequence of the following result of S. S. Pillai [2], obtained in quite a different way: if $g(x)$ denotes the number of natural numbers $m \leqslant x$ for which the equation $\varphi(n) = m$ is solvable, then $\lim\limits_{x \to \infty} \dfrac{g(x)}{x} = 0$.

In fact, as shown by H. Maier and C. Pomerance [1] there exists a real number $C = 0{,}81781465\ldots$ such that for every $\varepsilon > 0$ and $x > x_0(\varepsilon)$

$$\frac{x}{\log x} \exp\left((C-\varepsilon)(\log\log\log x)^2\right) < g(x)$$

$$< \frac{x}{\log x} \exp\left((C+\varepsilon)(\log\log\log x)^2\right).$$

It follows from Theorem 4 that for every natural number m the number of solutions of the equation $\varphi(n) = m$ in natural numbers n is finite $\geqslant 0$. Conversely, Theorem 4 is an immediate consequence of this fact. The theorem of Pillai implies the following:

THEOREM 6. *For every natural number s there exists a natural number m such that the equation $\varphi(n) = m$ has more than s different solutions in natural numbers n.*

PROOF. We give an elementary proof of this theorem, due to A. Schinzel [5]. Let s denote a natural number and let $m = (p_1 - 1)(p_2 - 1)\ldots(p_s - 1)$, where p_i is the ith prime. We are going to prove that each of the numbers $x_1, x_2, \ldots, x_{s+1}$, where $x_i = p_1 \ldots p_{i-1}(p_i - 1)p_{i+1} \ldots p_s$, $i = 1, 2, \ldots s$; $x_{s+1} = p_1 p_2 \ldots p_s$ is a solution of the equation $\varphi(n) = m$.

In fact, let i be one of the numbers $1, 2, \ldots, s$. The number $p_i - 1$ is not divisible by any prime $> p_i$, and so $p_i - 1 = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_{i-1}^{\gamma_{i-1}}$, where $\gamma_1, \gamma_2, \ldots, \gamma_{i-1}$ are non-negative integers. Hence $x_i = p_1^{\gamma_1+1} p_2^{\gamma_2+1} \ldots p_{i-1}^{\gamma_{i-1}+1} p_{i+1} p_{i+2} \ldots p_s$ and consequently

$$\varphi(x_i) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_{i-1}^{\gamma_{i-1}} (p_1 - 1)(p_2 - 1)\ldots(p_{i-1} - 1)(p_{i+1} - 1)\ldots(p_s - 1).$$

Hence, looking at the formula for $p_i - 1$ and recalling the definition of m, we see that $\varphi(x_i) = m$ for $i = 1, 2, \ldots, s$. Plainly, we also have $\varphi(x_{s+1}) = m$. We see that the numbers $x_1, x_2, \ldots, x_{s+1}$ are different and that they are positive integers; the theorem is thus proved. ☐

As has been shown by P. Erdös [3], there exists an infinite increasing sequence of natural numbers m_k ($k = 1, 2, \ldots$) such that the number of solutions of the equation $\varphi(n) = m_k$ for any $k = 1, 2, \ldots$ is greater than m_k^c, where c is a positive constant. A conjecture of P. Erdös is that for any number $\varepsilon > 0$ the constant in question can be taken equal to $1-\varepsilon$. A. Balog [1] has proved that this holds for $\varepsilon = \frac{7}{20}$.

The question arises whether for every natural number s there exists a natural number m such that the equation $\varphi(n) = m$ has precisely s solutions in natural numbers. We do not know the answer to this question even in the simple case of $s = 1$. In fact, we do not know any natural number m such that the equation $\varphi(n) = m$ has precisely one solution in natural numbers n. A conjecture of Carmichael [5] is that there is no such natural number m. As was shown by P. Masai and A. Valette [1], there are no such numbers $m \leqslant 10^{10000}$.

However, it can be proved that there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely two (or precisely three) solutions in natural numbers n (cf. Exercise 12 below).

For a natural number $s > 1$ denote by m_s the least natural number m such that the equation $\varphi(n) = m$ has precisely s solutions in natural numbers n (provided the number m_s exists). It can be calculated that $m_2 = 1$, $m_3 = 2$, $m_4 = 4$, $m_5 = 8$, $m_6 = 12$, $m_7 = 32$, $m_8 = 36$, $m_9 = 40$, $m_{10} = 24$, $m_{11} = 48$, $m_{12} = 160$, $m_{13} = 396$, $m_{14} = 2268$, $m_{15} = 704$.

We conjecture that for every natural number $s > 1$ there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely s solutions in natural numbers n. This follows from the Conjecture H (cf. Schinzel [13]). The main defficulty consists in proving the existence of the number m_s, since, as has been proved by P. Erdős [14], if for a given natural number s there exists a natural number m such that the equation $\varphi(n) = m$ has precisely s solutions (in natural numbers n), then there exist infinitely many natural numbers m with this property.

We do not know whether there exist infinitely many natural numbers which are not of the form $n - \varphi(n)$ where n is a natural number. (It can be proved that the numbers 10, 26, 34 and 50 are not of this form.) We do not know whether every odd number is of this form. (The answer is in the positive, provided any even natural number > 6 is the sum of two different prime numbers.)

EXERCISES. **1.** Prove the formula of N.C. Scholomiti [1]:

$$\varphi(n) = \sum_{k=1}^{n-1} \left[\frac{1}{(n,k)}\right] \text{for natural numbers } n > 1.$$

The proof follows from the remark that if $n > 1$, $k < n$ and $(n, k) = 1$, then $\left[\frac{1}{(n,k)}\right] = 1$. On the other hand, if $(n, k) > 1$, then $\left[\frac{1}{(n,k)}\right] = 0$. Therefore the right-hand side of the formula is equal to the number of natural numbers $< n$ relatively prime to n, which, for $n > 1$, is the value of $\varphi(n)$.

2. Find the natural numbers n for which $\varphi(n)$ is not divisible by 4.

SOLUTION. They are the numbers 1, 2, 4 and the numbers p^α and $2p^\alpha$, where p is a prime of the form $4t+3$. The proof is straightforward (cf. Carmichael [1], Klee [1]).

3. Prove that there exist infinitely many pairs of natural numbers $x, y, y > x$, such that $d(x) = d(y)$, $\varphi(x) = \varphi(y)$ and $\sigma(x) = \sigma(y)$.

PROOF. As is easy to see, all the equations are satisfied by the numbers $x = 3^k \cdot 568$, $y = 3^k \cdot 638$, where $k = 0, 1, 2, \ldots$ (cf. Jankowska [1]). ☐

4. Prove that there exist infinitely many systems x, y, z such that $x < y < z$ and $d(x) = d(y) = d(z)$, $\varphi(x) = \varphi(y) = \varphi(z)$, $\sigma(x) = \sigma(y) = \sigma(z)$.

PROOF. We put

$$x = 5^k \cdot 2^3 \cdot 3^3 \cdot 71 \cdot 113, \qquad y = 5^k \cdot 2^3 \cdot 3 \cdot 29 \cdot 37 \cdot 71,$$
$$z = 5^k \cdot 2 \cdot 3^3 \cdot 11 \cdot 29 \cdot 113. \quad \square$$

P. Erdös [15] has proved that for any natural number s there exist s different natural numbers $a_1, a_2, \ldots, a_s$ such that

$$d(a_i) = d(a_j), \qquad \varphi(a_i) = \varphi(a_j), \qquad \sigma(a_i) = \sigma(a_j)$$

hold for any $1 \leqslant i \leqslant j \leqslant s$. According to a conjecture of P. Erdös one may additionally assume that any two numbers of the sequence $a_1, a_2, \ldots, a_s$ are relatively prime (cf. Erdös [16]). ☐

5. Prove that for any natural number m there exists a natural number n such that

$$\varphi(n) - \varphi(n-1) > m \qquad \text{and} \qquad \varphi(n) - \varphi(n+1) > m.$$

PROOF. Let p be a prime of the form $4k+3$ that is greater than $2m+3$. Then, since $p = 4k+3$, we have $\varphi(p) = 4k+2$, $\varphi(p-1) = \varphi(4k+2) = \varphi(2k+1) \leqslant 2k+1$. Therefore $\varphi(p) - \varphi(p-1) \geqslant 2k+1 > m$. We also have $p+1 = 4(k+1) = 2^\alpha l$, where $\alpha \geqslant 2$ and l is an odd number. Hence

$$\varphi(p+1) = 2^{\alpha-1}\varphi(l) \leqslant 2^{\alpha-1} l = \tfrac{1}{2}(p+1),$$

and so

$$\varphi(p) - \varphi(p+1) \geqslant p - 1 - \tfrac{1}{2}(p+1) = \tfrac{1}{2}(p-3) > m. \quad \square$$

Let us mention the following fact: there exists a natural number $n > 1$ such that $\varphi(n-1)/\varphi(n) > m$ and $\varphi(n+1)/\varphi(n) > m$, and similarly there exists a natural number $n > 1$ such that $\varphi(n)/\varphi(n-1) > m$ and $\varphi(n)/\varphi(n+1) > m$ (cf. Schinzel and Sierpiński [1]).

It can be also proved (cf. Erdös and Schinzel [1]) that for any two natural numbers m and $k > 1$ there exist a natural number n such that

$$\frac{\varphi(n+i)}{\varphi(n+i-1)} > m \qquad \text{for} \qquad i = 1, 2, \ldots, k$$

and a natural number n such that

$$\frac{\varphi(n+i-1)}{\varphi(n+i)} > m \qquad \text{for} \qquad i = 1, 2, \ldots, k.$$

6. Prove that for arbitrary natural numbers a, b there exist infinitely many pairs of natural numbers x, y such that

$$\varphi(x):\varphi(y)=a:b.$$

PROOF. Let a and b be two given natural numbers. Without loss of generality we may assume that they are relatively prime. Let c denote a natural number prime to ab (there are of course infinitely many such numbers; in particular all the numbers $kab+1$, where $k=1,2,\ldots$, have this property). Let $x=a^2bc$, $y=ab^2c$. Since any two of the numbers a, b, c are relatively prime, $\varphi(x)=\varphi(a^2)\varphi(b)\varphi(c)$ and $\varphi(y)=\varphi(a)\varphi(b^2)\varphi(c)$. As follows easily from Theorem 3, for any natural number n we have $\varphi(n^2)=n\varphi(n)$, consequently $\varphi(a^2)=a\varphi(a)$, $\varphi(b^2)=b\varphi(b)$, whence $\varphi(x):\varphi(y)=a:b$, as required. ☐

It is worth observing that Conjecture H implies the existence of infinitely many primes x, y such that $\varphi(x):\varphi(y)=a:b$ for a given pair of natural numbers a, b (cf. Schinzel and Sierpiński [3], p. 192).

7. Prove that if n is a natural number >1, then there exist infinitely many natural numbers m such that $\varphi(m)/m=\varphi(n)/n$.

PROOF. Number n, being a natural number >1, has a prime divisor p; so we may assume that $n=p^{\alpha}n_1$, where α is a natural number and $(n_1,p)=1$. Hence

$$\frac{\varphi(n)}{n}=\frac{p^{\alpha-1}(p-1)\varphi(n_1)}{p^{\alpha}n_1}=\frac{p-1}{p}\cdot\frac{\varphi(n_1)}{n_1}.$$

Let $m=p^{\beta}n_1$, where β is a natural number. By a similar reasoning, we find

$$\frac{\varphi(m)}{m}=\frac{p-1}{p}\cdot\frac{\varphi(n_1)}{n_1},\quad\text{so}\quad\frac{\varphi(m)}{m}=\frac{\varphi(n)}{n},$$

and hence the claim follows. ☐

It can be proved that the numbers $\varphi(n)/n$, $n=1,2,\ldots$, form a dense subset in the unit interval $(0,1)$. On the other hand, there exists a dense subset of the interval $(0,1)$ consisting of rational numbers which are not of the form $\varphi(n)/n$ (cf. Schoenberg [1], Sierpiński [26], p. 210).

K. Zarankiewicz has raised a question whether the set of the numbers $\varphi(n+1)/\varphi(n)$, $n=1,2,\ldots$, is dense in the set of the real numbers. A. Schinzel [3] has proved that the answer to this question is affirmative (cf. Erdös and Schinzel [1]).

8. Find all the solutions of the equation $\varphi(n)=\varphi(2n)$ in natural numbers.

ANSWER. Those are all the odd numbers.

9. Find all the solutions of the equation $\varphi(2n)=\varphi(3n)$ in natural numbers.

ANSWER. They are those even natural numbers which are not divisible by 3.

10. Find all the solutions of the equation $\varphi(3n)=\varphi(4n)$ in natural numbers n.

ANSWER. They are all those natural numbers which are not divisible by 2 or by 3.

11. Prove that for any natural number k there exists at least one natural number n such that $\varphi(n+k)=\varphi(n)$.

PROOF. If k is an odd number, then the assertion holds, since in this case $\varphi(2k)=\varphi(k)$ and we may put $n=k$. Suppose that k is even, and let p denote the least prime which is not a divisor of k. Consequently each prime number $< p$ is a divisor of the number k. Hence $\varphi((p-1)k) = (p-1)\varphi(k)$ (this follows at once from Theorem 3 – in fact, if m is a natural number such that any prime divisor of it is a divisor of a natural number k, then $\varphi(mk) = m\varphi(k)$). But, since $(p,k) = 1$, we have $\varphi(pk) = \varphi(p)\varphi(k) = (p-1)\varphi(k) = \varphi((p-1)k)$, and so putting $n = (p-1)k$, we obtain $\varphi(n+k) = \varphi(n)$, as required (cf. Sierpiński [18], p. 184). □

It has been proved that for any natural number m there exists a natural number k such that the equation $\varphi(n+k) = \varphi(n)$ has more than m solutions in natural numbers n (cf. ibid. pp. 184–185).

12. Prove that there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely two solutions in natural numbers n.

PROOF. Such are for instance the numbers $m = 2\cdot 3^{6k+1}$, where $k = 1, 2, \ldots$ In fact, suppose that n is a natural number such that $\varphi(n) = 2\cdot 3^{6k+1}$. Of course, number n is not a power of number 2 (because $\varphi(2^\alpha) = 2^{\alpha-1}$); consequently it must have an odd prime divisor p, and moreover, it cannot have more than one such divisor, because $\varphi(n)$ is not divisible by 4.

If $p = 3$, then $n = 3^\beta$ or $n = 2^\alpha\cdot 3^\beta$, where α and β are natural numbers. Then, by $\varphi(n) = 2\cdot 3^{6k+1}$, we obtain $2\cdot 3^{\beta-1} = 2\cdot 3^{6k+1}$ or $2^\alpha\cdot 3^{\beta-1} = 2\cdot 3^{6k+1}$. Consequently, $\alpha = 1$ and, in either case, $\beta - 1 = 6k+1$. Therefore $n = 3^{6k+2}$ or $n = 2\cdot 3^{6k+2}$ and, as is easy to verify, in any case $\varphi(n) = 2\cdot 3^{6k+1} = m$.

If $p \neq 3$, that is if $p > 3$, then the number n cannot be divisible by p^2 because, if it were, $p \mid \varphi(n) = 2\cdot 3^{6k+1}$, which for $p > 3$ is impossible. Therefore $n = p$ or $n = 2^\alpha p$, where α is a natural number. Hence, by $\varphi(n) = 2\cdot 3^{6k+1}$ we find $p-1 = 2\cdot 3^{6k+1}$ or $2^{\alpha-1}(p-1) = 2\cdot 3^{6k+1}$. Consequently, since $p-1$ is even, $\alpha = 1$ and, in any case, $p = 2\cdot 3^{6k+1}+1$, which is impossible since, by $k \geqslant 1$, we have $p > 7$ and, in virtue of the theorem of Fermat, $3^6 \equiv 1 \pmod 7$, whence $p = 2\cdot 3^{6k+1}+1 \equiv 2\cdot 3+1 \equiv 0 \pmod 7$, so $7 \mid p$. Thus we see that the equation $\varphi(n) = 2\cdot 3^{6k+1}$, where k is a natural number, has precisely two solutions, $n = 3^{6k+2}$ and $n = 2\cdot 3^{6k+2}$. The equation $\varphi(n) = 2\cdot 3$, however, has four solutions: $n = 7$, 9, 14, 18, and the equation $\varphi(n) = 2\cdot 3^2$ also has four solutions: $n = 19, 27, 38, 54$. □

REMARK. A. Schinzel [6] has found infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely three solutions in natural numbers n. Such are, for instance the numbers $m = 7^{12k+1}\cdot 12$, where $k = 0, 1, 2, \ldots$ We then have $\varphi(n) = m$ for $n = 7^{12k+2}\cdot 3$, $7^{12k+2}\cdot 4$ and $7^{12k+2}\cdot 6$. The proof that there are no other solutions, though elementary, is rather long.

13. Find all the solutions of the equation $\varphi(n) = 2^{10}$ in natural numbers n.

SOLUTION. Suppose that n is an even number, and that $n = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_{k-1}^{\alpha_{k-1}}$ where $q_1, q_2, \ldots, q_{k-1}$ are odd primes, is the factorization of n into prime factors. Let $q_1 < q_2 < \ldots < q_{k-1}$. (We do not exclude the case $k = 1$, i.e. $n = 2^\alpha$). Since $\varphi(n) = 2^{10}$, we see that

$$2^{\alpha-1} q_1^{\alpha_1-1} q_2^{\alpha_2-1} \ldots q_{k-1}^{\alpha_{k-1}-1} (q_1-1)(q_2-1)\ldots(q_{k-1}-1) = 2^{10},$$

which proves that $\alpha_1 = \alpha_2 = \ldots = \alpha_{k-1} = 1$ and $q_i = 2^{\beta_i}+1$, $i = 1, 2, \ldots, k-1$, where β_i $(i = 1, 2, \ldots, k-1)$ are natural numbers, and, finally, $\alpha - 1 + \beta_1 + \beta_2 + \ldots + \beta_{k-1} = 10$, and so $\beta_i \leqslant 10$ for $i = 1, 2, \ldots, k-1$.

Odd prime numbers of the form $2^\beta+1$, $\beta \leqslant 10$ are the numbers $2^\beta+1$ with $\beta = 1, 2, 4, 8$ only. Therefore $k \leqslant 5$.

If $k = 1$ that is if $n = 2^\alpha$, then $\alpha - 1 = 10$, whence $\alpha = 11$ and consequently $n = 2^{11} = 2048$.

If $k = 2$, then $\alpha - 1 + \beta_1 = 10$ and for $\beta_1 = 1, 2, 4, 8$ we find $\alpha = 10, 9, 7, 3$, respectively. So the values for n are $2^{10} \cdot 3 = 3072$, $2^9 \cdot 5 = 2560$, $2^7 \cdot 17 = 2176$ or $2^3 \cdot 257 = 2056$.

If $k = 3$, then $\alpha - 1 + \beta_1 + \beta_2 = 10$. Here β_1 cannot be > 2 because, if it were, β_1 would be greater than or equal to 4. But, since $\beta_1 < \beta_2$ (for $q_1 < q_2$), we would obtain $\beta_2 > 4$ so $\beta_2 \geqslant 8$ and $\beta_1 + \beta_2 \geqslant 12$, which is impossible. Therefore β_1 is equal either to 1 or to 2. If $\beta_1 = 1$, then $\alpha + \beta_2 = 10$ and $\beta_2 > \beta_1 = 1$; so $\beta_2 = 2, 4$ or 8, which implies $\alpha = 8, 6, 2$, and this gives the following values for n : $2^8 \cdot 3 \cdot 5$, $2^6 \cdot 3 \cdot 17$ or $2^2 \cdot 3 \cdot 257$. If $\beta_1 = 2$, then $\alpha + \beta_2 = 9$, $\beta_2 = 4$ or 8, whence $\alpha = 5$ or 1 and so $n = 2^5 \cdot 5 \cdot 17$ or $2 \cdot 5 \cdot 257$.

If $k = 4$, then $\alpha - 1 + \beta_1 + \beta_2 + \beta_3 = 10$. Since $\beta_1 < \beta_2 < \beta_3$ (which holds because $q_1 < q_2 < q_3$), in virtue of the fact that $\beta_1, \beta_2, \beta_3$ can be chosen from the numbers $1, 2, 4, 8$ only, we infer that $\beta_1 = 1, \beta_2 = 2, \beta_3 = 4$, which proves that $\alpha = 4$ and so $n = 2^4 \cdot 3 \cdot 5 \cdot 17$.

Finally, we see that the case $k = 5$ is impossible. This is because the equality $k = 5$, implies $\beta_1 = 1, \beta_2 = 2, \beta_3 = 4, \beta_4 = 8$, which contradicts the equality $\alpha - 1 + \beta_1 + \beta_2 + \beta_3 + \beta_4 = 10$.

Now suppose that n is odd. Then $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_{k-1}^{\alpha_{k-1}}$, where $q_1, q_2, \ldots, q_{k-1}$ are odd prime numbers and $q_1 < q_2 < \ldots < q_{k-1}$. By assumption, we have

$$q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \ldots q_{k-1}^{\alpha_{k-1} - 1} (q_1 - 1)(q_2 - 1) \ldots (q_{k-1} - 1) = 2^{10}.$$

Hence $\alpha_1 = \alpha_2 = \ldots = \alpha_{k-1} = 1$ and $q_i = 2^{\beta_i} + 1$ for $i = 1, 2, \ldots, k-1$. Moreover, $\beta_1 + \beta_2 + \ldots + \beta_{k-1} = 10$.

If $k = 2$, then $\beta_1 = 10$, which is impossible. If $k = 3$, then $\beta_1 + \beta_2 = 10$, whence we easily infer that $\beta_1 = 2$, $\beta_2 = 8$, and this gives $n = 5 \cdot 257$.

If $k = 4$, then $\beta_1 + \beta_2 + \beta_3 = 10$, which is impossible because $\beta_1, \beta_2, \beta_3$ are different numbers chosen out of the sequence $1, 2, 4, 8$. Similarly, $k \geqslant 5$ is impossible.

Thus we reach the final conclusion that the equation $\varphi(n) = 2^{10}$ has 12 solutions in natural numbers n, namely:

$n = 2^{11}, 2^{10} \cdot 3, 2^9 \cdot 5, 2^7 \cdot 17, 2^3 \cdot 257, 2^8 \cdot 3 \cdot 5, 2^6 \cdot 3 \cdot 17, 2^2 \cdot 3 \cdot 257, 2^5 \cdot 5 \cdot 17, 5 \cdot 257, 2 \cdot 5 \cdot 257, 2^3 \cdot 3 \cdot 5 \cdot 17$.

REMARK. It can be proved that for $0 \leqslant m \leqslant 31$ (m being an integer) the equation $\varphi(n) = 2^m$ has $m + 2$ solutions in natural numbers n. For $31 < m < 2^{20}$ the equation has always precisely 32 solutions. The proof is based on the fact that the numbers $2^{2^n} + 1$ $(5 \leqslant n < 20)$ are composite (1).

14. Prove that there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has at least one solution in natural numbers and such that any solution of the equation is even.

PROOF. Let $m = 2^{32 + 2^s}$, where $s = 6, 7, \ldots$ If there existed an odd natural number n such that $\varphi(n) = m$, then n would be the product of different odd prime factors which, in addition, would be of the form $F_k = 2^{2^k} + 1$. (The argument is that if p is a prime and $p \mid n$, then $p - 1 \mid \varphi(n) = m$, whence it follows that $p - 1$ is a natural power of 2, and so $p = F_k$). Suppose that they are the numbers $F_{k_1}, F_{k_2}, \ldots, F_{k_l}$. Then $2^{k_1} + 2^{k_2} + \ldots + 2^{k_l} = 2^5 + 2^s$, where $h_1, h_2, \ldots, h_k$ are different natural numbers. The number 2^5+2^s, where $s > 5$, admits only one representation as the sum of different powers of the number 2. Therefore one of the numbers $F_{h_1}, F_{h_2}, \ldots, F_{h_k}$ must be equal to F_5, which is impossible, since F_5 is a composite number. Thus we see that the equation $\varphi(n) = m$ has no solutions in odd natural numbers. If n is allowed to be even, a solution can be easily found, for example $\varphi(2^{33+2^8}) = m$. ☐

---

(1) Cf. Carmichael [1] for $m < 2^{10}$. For the numbers $2^{10} \leqslant m < 2^{20}$ the proof is analogous.

15. Prove that, if $p > 2$ and $2p+1$ are prime numbers, then for $n = 4p$ the equality $\varphi(n+2) = \varphi(n)+2$ holds.

PROOF. If the numbers $p > 2$ and $2p+1$ are prime, then $\varphi(4p) = \varphi(4)\varphi(p) = 2(p-1)$ and $\varphi(4p+2) = \varphi(2(2p+1)) = \varphi(2p+1) = 2p$, whence $\varphi(4p+2) = \varphi(4p)+2$. ☐

REMARK. It easily follows from Conjecture H (cf. Chapter III, § 8) that there exist infinitely many pairs of twin prime numbers; similarly, it follows from this conjecture that there exist infinitely many primes p for which the numbers $2p+1$ are also prime. Consequently, Conjecture H implies that there exist infinitely many odd and infinitely many even numbers n which satisfy the equation $\varphi(n+2) = \varphi(n)+2$.

2. Properties of Euler's totient function

Now for a given natural number n we are going to calculate the number of natural numbers $\leqslant n$ such that the greatest common divisor of any of them and n is equal to a number d (with $d \mid n$).

In order that the greatest common divisor of the numbers $m \leqslant n$ and n be d it is necessary and sufficient that $m = kd$, where k is a natural number $\leqslant n/d$ relatively prime to n/d. Consequently, the number of natural numbers $m \leqslant n$ which satisfy the condition $(m, n) = d$ is equal to the number of natural numbers $\leqslant n/d$ which are relatively prime to n/d, and so it is equal to $\varphi(n/d)$.

Thus we see that *in the sequence* $1, 2, \ldots, n$ *for every natural divisor d of the natural number n there are precisely $\varphi(n/d)$ natural numbers m such that $(m, n) = d$.*

Let $d_1, d_2, \ldots, d_s$ be all the natural divisors of a natural number n. The numbers $1, 2, \ldots, n$ can be divided into s classes by the rule that a number m belongs to the ith class if and only if $(n, m) = d_i$. The number of elements of the ith class is then $\varphi\left(\frac{n}{d_i}\right)$. Moreover, since the number of numbers in the sequence $1, 2, \ldots, n$ is equal to n, we obtain the formula

$$\varphi\left(\frac{n}{d_1}\right) + \varphi\left(\frac{n}{d_2}\right) + \ldots + \varphi\left(\frac{n}{d_s}\right) = n.$$

But, clearly, if d_i runs over the set of all natural divisors of number n, then $\frac{n}{d_i}$ runs over the same set of all natural divisors of n. Hence $\varphi(d_1)+\varphi(d_2)+\ldots+\varphi(d_s) = n$, i.e.

$$\sum_{d|n} \varphi(d) = n. \tag{8}$$

We have thus proved the following

THEOREM 7. *The sum of the values of Euler's totient function over the set of natural divisors of a natural number n is equal to n.*

Applying Dirichlet's multiplication (cf. Chapter IV, § 3) to the series $a_1+a_2+\ldots$ and $b_1+b_2+\ldots$, where, for real $s > 2$, $a_n = \varphi(n)/n^s$, $b_n = 1/n^s$ $(n = 1, 2, \ldots)$, we obtain by (8)

$$c_n = \sum_{d|n} a_d b_{\frac{n}{d}} = \sum_{d|n} \frac{\varphi(d)}{d^s}\cdot\frac{d^s}{n^s} = \frac{1}{n^s}\sum_{d|n}\varphi(d) = \frac{n}{n^s} = \frac{1}{n^{s-1}}\cdot$$

Hence $\sum_{n=1}^{\infty} c_n = \zeta(s-1)$ and so

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \quad \text{for} \quad s > 2.$$

By the use of (8) we can prove the identity of Liouville

$$\sum_{n=1}^{\infty} \frac{\varphi(n)x^n}{1-x^n} = \frac{x}{(1-x)^2} \quad \text{for} \quad |x| < 1.$$

It follows from Theorem 6 of § 10, Chapter IV, that Euler's totient function is the only function φ that satisfies Theorem 7. Formulae (8) and (37) of Chapter IV give together the formula

$$\varphi(n) = n\sum_{d|n}\frac{\mu(d)}{d} \tag{9}$$

valid for all natural numbers n. Plainly, formula (9) can be rewritten in the form

$$\varphi(n) = \sum_{kl=n} l\mu(k) \tag{10}$$

where the summation extends over all the pairs of natural numbers k and l such that $kl = n$. For $x \geqslant 1$ formula (10) gives

$$(11)\qquad \sum_{n=1}^{[x]} \varphi(n) = \sum_{kl\leqslant x} l\mu(k),$$

where $\sum\limits_{kl\leqslant x}$ denotes the sum extended over all the pairs of natural numbers k, l such that $kl \leqslant x$. But, clearly,

$$\sum_{kl\leqslant x} l\mu(k) = \sum_{k=1}^{[x]}\Big(\mu(k)\sum_{l=1}^{[x/k]} l\Big)$$

and since

$$\sum_{l=1}^{[x/k]} l = \frac{1}{2}\left[\frac{x}{k}\right]\left(\left[\frac{x}{k}\right]+1\right),$$

in virtue of formula (33) of Chapter IV, formula (11) gives

$$(12)\qquad \sum_{n=1}^{[x]} \varphi(n) = \frac{1}{2} + \frac{1}{2}\sum_{k=1}^{[x]}\left(\mu(k)\left[\frac{x}{k}\right]^2\right).$$

This formula can be used for calculating the sum of the consecutive values of the function φ as well as for finding the approximate value of that sum. Using the formula

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2} = \frac{6}{\pi^2},$$

proved in Chapter IV, § 10, one can prove that the ratio of the number $\sum\limits_{n=1}^{[x]}\varphi(n)$ to the number $3x^2/\pi^2$ tends to 1, as x increases to infinity.

A generalization of the function $\varphi(n)$ is the function $\varphi_k(n)$, defined for pairs of natural numbers k, n as the number of the sequences $a_1, a_2, \ldots, a_k$ consisting of k natural numbers $\leqslant n$ such that $(a_1, a_2, \ldots, a_k, n) = 1$.

It is easy to prove the theorem of C. Jordan [1] (pp. 95–97) stating that if $n = q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ is the factorization of the number n into prime factors, then

$$\varphi_k(n) = n^k\left(1-\frac{1}{q_1^k}\right)\left(1-\frac{1}{q_2^k}\right)\ldots\left(1-\frac{1}{q_s^k}\right) \quad\text{and}\quad \sum_{d\mid n}\varphi_k(d) = n^k.$$

Another generalization of the function φ is the function $\Phi_k(n)$ given by V. L. Klee, Jr. [3]. This is defined for natural numbers k and n as the number of numbers h that occur in the sequence $1, 2, \ldots, n$ and are such that number (h, n) is not divisible by the kth power of any number greater than 1.

It is easy to prove that if $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ is the factorization of the number n into prime factors, then

$$\Phi_k(n) = \prod_{\alpha_i < k} q_i^{\alpha_i} \prod_{\alpha_i \geqslant k} q_i^{\alpha_i - k}(q_i^k - 1).$$

We also have

$$\Phi_k(n) = n \prod_{\substack{q^k | n \\ q \text{prime}}} (1 - q^{-k}) \quad \text{and} \quad \sum_{d|n} \Phi_k(d^k) = n^k.$$

3. The theorem of Euler

Let $m > 1$ be a given natural number and let

(13) $$r_1, r_2, \dots, r_{\varphi(m)}$$

be the sequence of the natural numbers relatively prime to m less than m. Let a denote an arbitrary integer relatively prime to m. Denote by ϱ_k the remainder obtained by dividing the number ar_k by m $(k = 1, 2, \dots, \varphi(m))$. We then have

(14) $$\varrho_k \equiv ar_k (\operatorname{mod} m) \quad \text{for} \quad k = 1, 2, \dots, \varphi(m)$$

and

(15) $$\varrho_k = ar_k + mt_k,$$

where $t_k (k = 1, 2, \dots, \varphi(m))$ are integers.

We are going to prove that the numbers

(16) $$\varrho_1, \varrho_2, \dots, \varrho_{\varphi(m)}$$

and numbers (13) are identical in certain order. For this purpose it is sufficient to prove that

(i) any term of sequence (16) is a natural number relatively prime to m and less than m,

(ii) the elements of sequence (16) are different.

Let $d_k = (\varrho_k, m)$. In virtue of (15), we see that $ar_k = \varrho_k - mt_k$, whence it follows that $d_k \mid ar_k$. But, since $(a, m) = (r_k, m) = 1$, $(ar_k, m) = 1$. Therefore, in view of $d_k \mid m$ and $d_k \mid ar_k$, we must have $d_k = 1$, i.e. $(\varrho_k, m) = 1$. On the other hand, number ϱ_k, as the remainder obtained from division by m, satisfies the inequalities $0 \leqslant \varrho_k < m$. Moreover, since $(\varrho_k, m) = 1$ and $m > 1$, ϱ_k cannot be equal to 0. Thus we have proved that the terms of sequence (16) have property (i).

Now, suppose that for certain two different indices i and j taken out of the sequence $1, 2, \ldots, \varphi(m)$ the equality $\varrho_i = \varrho_j$ holds. Then, in virtue of (14), we have $ar_i \equiv ar_j \pmod{m}$, and so $m \mid a(r_i - r_j)$ and, since $(a, m) = 1$, we have $m \mid r_i - r_j$, which is impossible because r_i and r_j, as two different terms of sequence (13), (since $i \neq j$) are different natural numbers $\leqslant m$. We have thus proved that the terms of sequence (16) have property (ii).

This proves that the elements of sequence (16) and those of sequence (13) are identical apart from the order. Therefore

$$\varrho_1 \varrho_2 \ldots \varrho_{\varphi(m)} = r_1 r_2 \ldots r_{\varphi(m)}.$$

Denote by P the common value of these products. The number P is relatively prime to m because anyone of its factors is relatively prime to m.

Multiplying the congruences obtained from (14) by substituting $1, 2, \ldots, \varphi(m)$ for k, we obtain

$$\varrho_1 \varrho_2 \ldots \varrho_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \pmod{m},$$

that is, the congruence $P \equiv a^{\varphi(m)} P \pmod{m}$ which is, clearly, equivalent to $m \mid P(a^{\varphi(m)} - 1)$, whence, since $(P, m) = 1$, we obtain $m \mid a^{\varphi(m)} - 1$.

We have thus proved

THEOREM 8 (Euler). *For any integer a which is relatively prime to a natural number m the congruence*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

holds.

If p is a prime, then $\varphi(p) = p - 1$; therefore the theorem of Euler can be regarded as a generalization of the theorem of Fermat (proved in Chapter V, § 5).

THEOREM 8^a (Rédei) (¹). *For any natural number $m > 1$ and every integer a we have*

$$m \mid a^m - a^{m - \varphi(m)}. \tag{17}$$

PROOF. Let $m = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ be the factorization of the number m into prime factors. Let i denote one of the numbers $1, 2, \ldots, k$. If $(a, q_i) = 1$,

---

(¹) Cf. Szele [1], footnote 2.

then, in view of Theorem 8, we have $q_i^{\alpha_i} \mid a^{\varphi(q_i^{\alpha_i})}-1$, and, since by Theorem 3 $\varphi(q_i^{\alpha_i}) \mid \varphi(m)$, we have $q_i^{\alpha_i} \mid a^{\varphi(m)}-1$.

If α and $q \geqslant 2$ are natural numbers, then (as it is easy to prove by induction) $q^{\alpha-1} \geqslant \alpha$. On the other hand, for $i = 1, 2, \ldots, k$, we have $q_i^{\alpha_i-1} \mid m$ and $q_i^{\alpha_i-1} \mid \varphi(m)$, whence $q_i^{\alpha_i-1} \mid m-\varphi(m)$. Since, moreover, $m-\varphi(m)$ is positive for m greater than 1, the last relation implies that $m-\varphi(m) \geqslant q_i^{\alpha_i-1} \geqslant \alpha_i$. Hence, in the case where $(a, q_i) > 1$, that is, if $q_i \mid a$, we have $q_i^{\alpha_i} \mid q_i^{m-\varphi(m)} \mid a^{m-\varphi(m)}$.

Thus we see that for any integer a the relation $q_i^{\alpha_i} \mid a^{m-\varphi(m)}(a^{\varphi(m)}-1)$ holds for every $i = 1, 2, \ldots, k$. This means that $q_i^{\alpha_i} \mid a^m - a^{m-\varphi(m)}$, whence, looking at the factorization of a into prime factors, we see that formula (17) holds. Theorem 8^{a} is thus proved. □

The theorem of Euler is an easy consequence of Theorem 8^{a}. In fact, in view of Theorem 8^{a}, for any natural $m > 1$ and any integer a we have $m \mid a^{m-\varphi(m)}(a^{\varphi(m)}-1)$. So, if in addition $(a, m) = 1$, then $(a^{m-\varphi(m)}, m) = 1$, whence $m \mid a^{\varphi(m)}-1$, which gives the theorem of Euler.

EXERCISES. **1.** Prove that from any infinite arithmetical progression, whose terms are integers, a geometric progression can be selected.

PROOF. Suppose we are given an infinite arithmetical progression

$$a, a+r, a+2r, \ldots \tag{18}$$

the terms of which are integers. If $r = 0$, there is nothing to prove since then the whole sequence (18) can be regarded as a geometric progression.

If $r < 0$, the desired result follows provided it is proved for the arithmetical progression obtained from the original one by a simple change of the sign at each of the terms of the progression. Thus the problem reduces to the case where r is a natural number. Moreover, we may suppose that $(a, r) = 1$, since otherwise, that is, if $d = (a, r) > 1$, we have $a = da'$, $r = dr'$ where $(a', r') = 1$, and so it is sufficient to prove the theorem for the arithmetic progression $a', a'+r', a'+2r', \ldots$

Finally, since $r > 0$, from a certain term onwards all the terms of (18) are greater than 1. Thus in order to prove the theorem we may remove some terms at the beginning and suppose $a > 1$. Since $(a, r) = 1$, then, by Theorem 8, we have $a^{\varphi(r)} \equiv 1 \pmod{r}$. Hence, for natural numbers $n, a^{n\varphi(r)} \equiv 1 \pmod{r}$ and therefore the number $k_n = (aa^{n\varphi(r)}-a)/r$ is an integer for any $n = 1, 2, \ldots$ But $a+k_n r = a(a^{\varphi(r)})^n$ for $n = 1, 2, \ldots$, and so, since $a > 0$, $0 \leqslant k_1 < k_2 < \ldots$ and the numbers $a+k_n r$ $(n = 1, 2, \ldots)$ form a geometrical progression. □

The theorem we have just proved implies that in any infinite arithmetical progression there are infinitely many terms which have the same prime factors (cf. Pólya and Szegö [1], p. 344). Another consequence of the theorem just proved is this: from any infinite arithmetical progression whose terms are rational numbers an infinite geometric progression can be selected.

2. Prove that if m, a, r are natural numbers with $(a, r) = 1$ and Z is any infinite set of terms of the arithmetical progression $a+kr\,(k = 1, 2, \ldots)$, then the progression contains terms which are products of more than m different numbers of the Z.

PROOF. We take $s = m\varphi(r)+1$ different numbers of the set Z. Denote them by $t_1, t_2, \ldots, t_s$. These numbers, being the terms of the arithmetical progression $a+kr\,(k = 1, 2, \ldots)$, are congruent to $a \pmod r$. So $t_1 t_2 \ldots t_s \equiv a^s \equiv a \cdot a^{m\varphi(r)} \pmod r$, whence, in view of $(a, r) = 1$, by Theorem 8, we infer that $a^{\varphi(r)} \equiv 1 \pmod r$. Therefore $t_1 t_2 \ldots t_s \equiv a \pmod r$, and consequently the number $t_1 t_2 \ldots t_s$ is a term of the arithmetical progression $a+kr\,(k = 1, 2, \ldots)$ Moreover, $s = m\varphi(r)+1 > m$, and so the proof follows. ☐

3. Prove that every natural number which is not divisible by 2 or by 5 is a divisor of a natural number whose digits (in the scale of ten) are all equal to 1.

PROOF. If $(n, 10) = 1$, then of course $(9n, 10) = 1$ and hence, by Theorem 8, $10^{\varphi(9n)} \equiv 1 \pmod{9n}$. Therefore $10^{\varphi(9n)}-1 = 9nk$, where k is a natural number. Hence $nk = (10^{\varphi(9n)}-1)/9$ and thus we see that the digits (in the scale of ten) of this number are equal to 1. ☐

4. Prove that every natural number has a multiple whose digits (in the scale of ten) are all equal to 1 or 0 and the digits equal to 1 precede those equal to 0.

PROOF. Every natural number can be represented in the form $n = n_1 2^\alpha 5^\beta$, where $(n_1, 10) = 1$. In virtue of Exercise 3, the number n_1 is a divisor of a number m whose digits (in the scale of ten) are equal to 1. On the other hand, $2^\alpha 5^\beta \mid 10^\gamma$, where $\gamma = \max(\alpha, \beta)$; consequently, $n \mid m \cdot 10^\gamma$. ☐

5. Find all the solutions of the congruence $x^x \equiv 3 \pmod{10}$ in natural numbers x.

SOLUTION. If a natural number x satisfies the congruence, then, since $(3, 10) = 1$, we must have $(x, 10) = 1$. Consequently $(x+20k, 10) = 1$ for any $k = 0, 1, 2, \ldots$ Hence, by Theorem 8, since $\varphi(10) = 4$, we find that $(x+20k)^4 \equiv 1 \pmod{10}$ and, *a fortiori*, $(x+20k)^{20k} \equiv 1 \pmod{10}$. On the other hand, the congruence $(x+20k)^x \equiv x^x \pmod{10}$ holds for any natural number x. Therefore, multiplying the last two congruences, we obtain $(x+20k)^{x+20k} \equiv x^x \pmod{10}$ for any $k = 0, 1, 2, \ldots$ If a natural number x satisfies the congruence $x^x \equiv 3 \pmod{10}$, then any of the terms of the arithmetic progression $x+20k\,(k = 0, 1, 2\ldots)$ just obtained also satisfies it. It is easy to verify that among the integers x such that $0 \leqslant x < 20$ only numbers 7 and 13 satisfy the congruence. From this we infer that the solutions of the congruence $x^x \equiv 3 \pmod{10}$ in natural numbers x are precisely the numbers $7+20k$ and $13+20k$, where $k = 0, 1, 2, \ldots$

4. Numbers which belong to a given exponent with respect to a given modulus

It follows from Theorem 8 that if a is an integer relatively prime to a natural number m, then the congruence

$$a^x \equiv 1 \pmod m \tag{19}$$

has infinitely many solutions in natural numbers x; for example an infinite set of solutions is formed by the numbers $x = k\varphi(m)$, where $k = 1, 2, \ldots$ On the other hand, it is clear that congruence (19) has natural solutions only in the case where $(a, m) = 1$.

If $x = \delta$ is the least natural solution of congruence (19), then we say that *number a belongs to exponent δ with respect to modulus m.*

It is clear that if two numbers are congruent with respect to modulus m, then they belong to the same exponent with respect to modulus m; for if $a \equiv b \pmod{m}$ and for some x formula (19) holds, then $b^x \equiv 1 \pmod{m}$ (since, as we know, the congruence $a \equiv b \pmod{m}$ implies the congruence $a^x \equiv b^x \pmod{m}$ for any $x = 1, 2, \ldots$).

THEOREM 9. *If $(a, m) = 1$, then any solution of congruence* (19) *is divisible by the exponent δ to which a belongs with respect to modulus m.*

PROOF. Suppose, to the contrary, that the solution x of congruence (19) is not divisible by δ. This means that x divided by δ leaves a positive remainder r. Accordingly, $x = k\delta + r$, where k is a non-negative integer. By (19) we have

$$(20) \qquad a^{k\delta+r} \equiv 1 \pmod{m} \qquad \text{that is} \qquad (a^{\delta})^k a^r \equiv 1 \pmod{m}.$$

By the definition of δ the congruence $a^{\delta} \equiv 1 \pmod{m}$ holds. Therefore, by (20), $a^r \equiv 1 \pmod{m}$. Thus we see that our assumption leads us to the conclusion that there exists a solution r of congruence (19) less than δ, which contradicts the definition of δ. The theorem is thus proved. □

Since, by Theorem 8, $\varphi(m)$ is a solution of congruence (19), Theorem 9 implies the following

COROLLARY. *The exponent to which an arbitrary number relatively prime to m belongs with respect to modulus m is a divisor of the number $\varphi(m)$.*

In particular, numbers (relatively prime to m) which belong to exponent $\varphi(m)$ with respect to modulus m (that is numbers which belong to the maximum exponent with respect to modulus m), if they exist, are called *primitive roots of the number m.*

For example, 3 is a primitive root of the number 10 because $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1 \pmod{10}$ and $\varphi(10) = 4$. The number 10, however, is not a primitive root of the number 3 because $10 \equiv 1 \pmod{3}$, which shows that 10 belongs to the exponent 1 with respect to modulus 3 and $\varphi(3) = 2$.

Number 7 is also a primitive root of the number 10 since $7^1 \equiv 7$, $7^2 \equiv 9$, $7^3 \equiv 3$, $7^4 \equiv 1 \pmod{10}$. Equally, 10 is a primitive root of the number 7 because $10 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, $10^6 \equiv 1 \pmod 7$ and $\varphi(7) = 6$.

It follows immediately from Theorem 8 that for any natural number m there exists the least natural number $\lambda(m)$ such that $m \mid a^{\lambda(m)} - 1$ for $(a, m) = 1$(¹). Number $\lambda(m)$ is called the *minimum universal exponent* mod m. By Theorem 8, the inequality $\lambda(m) \leqslant \varphi(m)$ holds for any natural m. It can be proved that $\lambda(2) = 1$, $\lambda(2^2) = 2$, $\lambda(2^\alpha) = 2^{\alpha-2}$, $\alpha = 3, 4, \ldots$ It is also true that if $m = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$, $2 < q_1 < q_2 < \ldots < q_s$ is the factorization of number m into prime factors, then

$$\lambda(m) = [\lambda(2^{\alpha_0}), \varphi(q_1^{\alpha_1}), \ldots, \varphi(q_s^{\alpha_s})],$$

and that for any natural number m there exist natural numbers that belongs to the exponent $\lambda(m)$ with respect to modulus m (cf. Ore [1], pp. 292–293).

As announced in Mathematical Tables and other Aids to Computation 4 (1950), pp. 29-30, S. Whitten [1] has tabulated the function $\lambda(n)$ for $n \leqslant 1200$.

The accompanying table covers the values of the function $\lambda(m)$ for $m < 100$.

	0	1	2	3	4	5	6	7	8	9
			1	2	2	4	2	6	2	6
1	4	10	2	12	6	4	4	16	6	18
2	4	6	10	22	2	20	12	18	6	28
3	4	30	8	10	16	12	6	36	18	12
4	4	40	6	42	10	12	22	46	4	42
5	20	16	12	52	18	20	6	18	28	58
6	4	60	30	6	16	12	10	66	16	22
7	12	70	6	72	36	20	18	30	12	78
8	4	54	40	82	6	16	42	28	10	88
9	12	12	22	30	46	36	8	96	42	30

It can be proved that $\lambda(m) = \varphi(m)$ holds only for $m = 1, 2, 4, p^\alpha$ and $2p^\alpha$, where p is an odd prime and α a natural number. Another fact worth reporting is that there exists an increasing infinite sequence of natural

---

(¹) This function should not be mistaken for the function of Liouville considered in Chapter IV, § 11.

numbers $n_k\,(k = 1, 2, \ldots)$ such that $\lim_{k=\infty} \lambda(n_k)/\varphi(n_k) = 0$. For example, such is the sequence $n_k = p_1 p_2 \ldots p_k\,(k = 1, 2, \ldots)$. It can also be proved that in order that a number m be a composite number of Carmichael (and so absolutely pseudo-prime) it is necessary and sufficient that $\lambda(m) \mid m-1$ (cf. Carmichael [2], p. 237, formula (18)).

As announced by Carmichael (ibid., p. 236) the equation $\lambda(n) = 2$ has precisely six solutions, $n = 3, 4, 6, 8, 12, 24$, and the equation $\lambda(n) = 4$ has 12 solutions (the least of which is $n = 5$ and the greatest $n = 240$); the equation $\lambda(n) = 12$ has 84 solutions (the least of which is $n = 13$ and the greatest $n = 65520$). We have $\lambda(100) = 20$. For $n < 100$ the equality $\lambda(n+1) = \lambda(n)$ holds only for $n = 3$, 15 and 90.

For every natural number s there exists a natural number m_s such that the equation $\lambda(n) = m_s$ has more than s solutions in natural numbers n. By Theorem 11, which will be proved in the next section, for every natural number s there exists a natural number k such that $p = 2^s k+1$ is a prime number. For $j = 0, 1, 2, \ldots, s, s+1$ we have $\lambda\left(2^j(2^s k+1)\right) = 2^s k$, so putting $m_s = 2^s k$ we obtain the desired result.

It is easy to prove that for natural numbers $n > 2$ the numbers $\lambda(n)$ are even. There exist infinitely many even numbers which are not values of the function $\lambda(n)$. It can be proved that the numbers $2 \cdot 7^k$, where $k = 1, 2, \ldots$, have this property (cf. Sierpiński [26], pp. 191–192).

THEOREM 10. *If p is a prime > 2, then any natural divisor of the number $2^p - 1$ is of the form $2kp+1$, where k is an integer.*

PROOF. Since the product of two (or more) numbers of the form $2kp+1$ is also of this form, and since 1 is of this form (for $k = 0$), it is sufficient to prove that every prime divisor q of the number 2^p-1 is of the form $2kp+1$. If $q \mid 2^p - 1$, then $2^p \equiv 1 \pmod{q}$ and so, by Theorem 9, $\delta \mid p$, where δ denotes the exponent to which the number 2 belongs with respect to modulus q. We cannot have $\delta = 1$ because, in that case, $2 \equiv 1 \pmod{q}$ and so $q \mid 1$, which is impossible. Therefore, since $\delta \mid p$ and p is a prime, we infer that $\delta = p$. On the other hand, the corollary to Theorem 9 gives $\delta \mid \varphi(q)$, i.e. $\delta \mid q-1$. Thus we see that $p \mid q-1$ and, since q is a divisor of an odd number and since $(p, 2) = 1$ (because p is a prime > 2), we conclude that $2p \mid q-1$, that is $q-1 = 2kp$, so $q = 2kp+1$, where k is an integer. The theorem is thus proved. □

We note that in Theorem 10 the assumption that p is a prime > 2 is essential; the divisors 3, 5 and 15 of the number 2^4-1 are not of the form $8k+1$ and the divisor $7 = 2^3-1$ of the number $2^{15}-1$ is not of the form $30k+1$.

EXERCISES. **1.** Prove the following theorem of Fermat:

If p is a prime > 3, then any natural divisor > 1 of the number $(2^p+1)/3$ is of the form $2kp+1$, where k is a natural number.

PROOF. The number $(2^p+1)/3$ is a natural number since, for odd p, $2+1 \mid 2^p+1$. Let d denote a divisor > 1 of number $(2^p+1)/3$ and let q be a prime divisor of d. If $q = 3$, then $2^p+1 \equiv 0 \pmod 9$, whence $2^{2p} \equiv 1 \pmod 9$ and, by Theorem 9, number $2p$ is divisible by the exponent to which number 2 belongs with respect to modulus 9. But, as is easy to calculate, $\delta = 6$, so $6 \mid 2p$, whence $3 \mid p$, and this contradicts the assumption that $p > 3$. Therefore, necessarily, $q \neq 3$. Since $2^p+1 \equiv 0 \pmod q$, we have $2^{2p} \equiv 1 \pmod q$. Now let δ denote the exponent to which number 2 belongs with respect to modulus q. We cannot have $\delta = 1$, or $\delta = 2$, because $q \neq 3$. Therefore $\delta > 2$. But, in virtue of Theorem 9, $\delta \mid 2p$ and, by $2^{q-1} \equiv 1 \pmod q$, $\delta \mid q-1$. Thus we see that numbers $2p$ and $q-1$ have a common divisor $\delta > 2$, which, in turn, implies that numbers p and $q-1$ have a common divisor > 1. But, since p is a prime, this implies that $p \mid q-1$ and so $q = pt+1$, where t is an integer and, in view of the fact that the numbers p, q are odd, t is even. Thus we conclude that $q = 2kp+1$, where k is a natural number, and so we see that each divisor of the number d is of the form $2kp+1$. Consequently the number d itself is of the form $2kp+1$. This completes the proof of the theorem. ☐

2. Prove that if a, b and n are natural numbers such that $a > b$, $n > 1$, then each prime divisor of the number a^n-b^n is either of the form $nk+1$, where k is an integer, or a divisor of the number $a^{n_1}-b^{n_1}$, where $n_1 \mid n$ and $n_1 < n$.

PROOF. Let $(a, b) = d$. Since $a > b$, we have $a = a_1 d, b = b_1 d$, where $(a_1, b_1) = 1$ and $a_1 > b_1$. Suppose that p is a prime divisor of number a^n-b^n. Then $p \mid a^n-b^n = d^n(a_1^n-b_1^n)$. If $p \mid d^n$, then $p \mid d$ and hence $p \mid a-b$, and the theorem is proved. Suppose that $p \mid a_1^n-b_1^n$. Then, since $(a_1, b_1) = 1$, we have $(a_1, p) = (b_1, p) = 1$. Let p be a primitive divisor of number $a_1^\delta-b_1^\delta$ (this means that $p \mid a_1^\delta-b_1^\delta$ and $p \nmid a_1^m-b_1^m$ for $0 < m < \delta$). We note that then $\delta \mid n$. In fact, suppose that n is not divisible by δ. Then $n = k\delta+r$, where k is an integer $\geqslant 0$ and $0 < r < \delta$. But $p \mid a_1^\delta-b_1^\delta$, and so $p \mid a_1^{k\delta}-b_1^{k\delta}$. In virtue of the identity

$$a_1^{k\delta+r}-b_1^{k\delta+r} = (a_1^{k\delta}-b_1^{k\delta})\,a_1^r+b_1^{k\delta}(a_1^r-b_1^r)$$

we have $p \mid b_1^{k\delta}(a_1^r-b_1^r)$, which, in view of $(b_1, p) = 1$, implies that $p \mid a_1^r-b_1^r$ for $0 < r < \delta$, contrary to the assumption that p is a primitive divisor of number $a_1^\delta-b_1^\delta$.

If $\delta < n$, then $\delta \mid n$ and $p \mid a_1^{n_1}-b_1^{n_1} \mid a^{n_1}-b^{n_1}$ for $n_1 = \delta$, $n_1 \mid n$ and $n_1 < n$. Let $\delta = n$. Then, in virtue of the theorem of Fermat, $p \mid a_1^{p-1}-1$, $p \mid b_1^{p-1}-1$, whence $p \mid a_1^{p-1}-b_1^{p-1}$. Consequently, $n = \delta \mid p-1$ and so p is of the form $nk+1$. ☐

3. Prove that, if a, b, n are natural numbers $a > b, n > 1$, then every prime divisor of the number a^n+b^n is of the form $2nk+1$, where k is an integer, or is a divisor of the number $a^{n_1}+b^{n_1}$, where n_1 is the quotient obtained by dividing the number n by an odd number greater than 1.

The proof is analogous to that in the preceding exercise.

5. Proof of the existence of infinitely many primes in the arithmetical progression $nk+1$

THEOREM 11. *If p is a prime and s a natural number, then there exist infinitely many primes of the form $2p^sk+1$, where k is a natural number.*

PROOF. Let p be a prime and let s be a natural number. We set $a = 2^{p^{s-1}}$. Let q denote an arbitrary prime divisor of number $a^{p-1}+a^{p-2}+ \dots a+1$. If a were congruent to $1 \pmod q$, then $q \mid a^{p-1}+a^{p-2}+ \dots +a+1 \equiv p \pmod q$; so $q \mid p$, which, in view of the fact that p and q are primes, would imply $q = p$, and so $a^p \equiv 1 \pmod p$, that is, $2^{p^s} \equiv 1 \pmod p$. But, in virtue of Theorem 5^a of Chapter V, we have $2^p \equiv 2 \pmod p$, whence, by induction, $2^{p^s} \equiv 2 \pmod p$, and this would show that 1 is congruent to $2 \pmod p$; so $p \mid 1$, which is impossible. We have thus proved that $a \not\equiv 1 \pmod q$, i.e. that $2^{p^{s-1}} \not\equiv 1 \pmod q$. Let δ denote the exponent to which 2 belongs with respect to modulus q. Since $q \mid a^p-1$, i.e. $2^{p^s} \equiv 1 \pmod q$, we see that $\delta \mid p^s$ and, since by $2^{p^{s-1}} \not\equiv 1 \pmod q$, the relation $\delta \mid p^{s-1}$ is impossible, δ must be equal to p^s. In virtue of the corollary to Theorem 9, we have $\delta \mid \varphi(q)$, i.e. $p^s \mid q-1$. By $2^{p^s} \equiv 1 \pmod q$, we see that number q is odd and, consequently, $p-1$ is even. If p is a prime > 2, then $(p, 2) = 1$ and so, in view of $p^s \mid q-1$, we see that $2p^s \mid q-1$, which shows that $q = 2p^sk+1$ for a natural number k. If $p = 2$, then $2^s \mid q-1$, whence $q = 2^sk+1$, where k is a natural number.

Thus we have proved that if p is odd, then there exists at least one prime number of the form $2p^sk+1$; if $p = 2$, then there exists at least one prime of the form 2^sk+1. Since s is arbitrary, this proves Theorem 11. □

The proof of a more general theorem is slightly more difficult:

THEOREM 11^a. *For any natural number n there exist infinitely many prime numbers of the form $nk+1$, where k is a natural number.*

PROOF (due to A. Rotkiewicz [4]) (cf. Estermann [2]). First we note that in order to prove the theorem it is sufficient to show that for any natural number n there exists at least one prime number of the form $nk+1$, where k is a natural number; for this implies that for any two natural numbers n, m there exists at least one prime of the form $nmt+1$, where t is a natural number, and this prime is, clearly, $> m$ and of the form $nk+1$ (where k is a natural number).

It is also plain that without loss of generality we may suppose that $n > 2$ (for in the sequence of odd numbers there exist (as we know) infinitely many primes).

Let $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ be the factorization of number n into prime factors with $q_1 < q_2 < \dots < q_s$.

Suppose that for any prime divisor p of number $a^n - 1$ number n belongs to an exponent $< n$ with respect to the modulus p. Let

$$P_n = \prod_{d|n} (n^d - 1)^{\mu(n/d)}, \tag{21}$$

where μ is the Möbius function (cf. Chapter IV, § 10). We represent each of the factors $n^d - 1$ as the product of its prime factors. Then product (21) becomes the product of prime factors; the exponent of any of them is an integer, positive, negative, or zero. Let p be one of those prime factors. Then there exists a natural number $d \mid n$ such that $p \mid n^d - 1$. Since $d \mid n$, then, *a fortiori*, $p \mid n^n - 1$ and $(n, p) = 1$. Let δ denote the exponent to which n belongs with respect to modulus p. It follows from the assumption that $\delta < n$. As an immediate consequence of Theorem 9, we see that among the numbers $n^d - 1$, where $d \mid n$, numbers divisible by p are precisely those for which $\delta \mid d$ holds, i.e. those for which $d = \delta k$, where k is a natural number such that $\delta k \mid n$, that is $k \mid \frac{n}{\delta}$. Since $p \mid n^n - 1$, we have $\delta \mid n$, whence we infer that n/δ is a natural number > 1 (because $\delta < n$).

Let λ be the greatest exponent for which p^λ divides $n^\delta - 1$. We have $p^\lambda \mid n^\delta - 1$ and $p^{\lambda+1} \nmid n^\delta - 1$. If for a natural number $k \mid n/\delta$ we have $p^{\lambda+1} \mid n^{k\delta} - 1$, then, by the identity

$$\frac{n^{\delta k} - 1}{n^\delta - 1} = \left((n^\delta)^{k-1} - 1\right) + \left((n^\delta)^{k-2} - 1\right) + \dots + (n^\delta - 1) + k,$$

$p \mid k$, which is impossible, since $k \mid n$ and $(n, p) = 1$. Therefore, for every natural number $k \mid n/\delta$, λ is the greatest exponent such that $p^\lambda \mid n^{\delta k} - 1$. From this we infer that in the factorization of number (21) the exponent of the prime p is $\sum_{k|\frac{n}{\delta}} \lambda \mu\left(\frac{n}{\delta k}\right)$. But, since n/δ is a natural number > 1, by formula (32) of Chapter IV, § 10, we see that $\sum_{k|\frac{n}{\delta}} \mu\left(\frac{n}{\delta k}\right) = \sum_{k|\frac{n}{\delta}} \mu(k) = 0$.

Since this is valid for any prime factor p of number (21), we see that $P_n = 1$. But by (21) we have

$$P_n = \prod_{d\mid n} (n^{n/d}-1)^{\mu(d)} = \prod_{d\mid q_1 q_2 \ldots q_s} (n^{n/d}-1)^{\mu(d)} \tag{22}$$

because, as we know, $\mu(d) = 0$ whenever d is divisible by the square of a natural number > 1. Let $b = n^{q_1^{\alpha_1-1} q_2^{\alpha_2-1} \ldots q_s^{\alpha_s-1}}$. We have $b \geqslant n > 2$ and $b^{q_1 q_2 \ldots q_s} = n^n$, thus, by (22)

$$P_n = \prod_{d\mid q_1 q_2 \ldots q_s} (b^{q_1 q_2 \ldots q_s/d}-1)^{\mu(d)}.$$

We see that P_n is the quotient of two polynomials in b with integral coefficients. Now we are going to find the least exponents of b that appear in the numerator and in the denominator of this quotient. We consider two cases separately: that of s being even and that of s being odd. In the former case the least natural exponent of b in the numerator is obtained for $d = q_1 q_2 \ldots q_s$. Consequently the exponent is equal to 1. As it is easy to see, the numerator divided by b^2 leaves a remainder equal either to $b-1$ or to b^2-b+1. In the denominator, however, in virtue of the inequalities $q_1 < q_2 < \ldots < q_s$, the least exponent is obtained for $d = q_2 q_3 \ldots q_s$. Consequently the exponent is equal to q_1. The denominator divided by b^2 yields the remainder 1 or b^2-1. But, since $P_n = 1$, this leads to a contradiction because, since $b > 2$, numbers $b-1$ and b^2-b+1 are different from numbers 1 and b^2-1. If s is odd, then the least exponent of b that appears in the numerator is obtained for $d = q_2 q_3 \ldots q_s$; the same for the denominator is obtained for $d = q_1 q_2 \ldots q_s$, which, as before, leads to a contradiction.

Thus, as we see, the assumption that for any prime divisor p of the number n^n-1 number n belongs to an exponent less than n with respect to modulus p leads to a contradiction.

Therefore number n^n-1 has at least one prime divisor p such that n belongs to the exponent n with respect to the modulus p. But $(n, p) = 1$, and so, by the theorem of Fermat, $p \mid n^{p-1}-1$, whence, by Theorem 9, $n \mid p-1$, i.e. $p = nk+1$, where k is a natural number.

We have thus shown that for every natural number $n > 1$ there exists at least one prime number of the form $nk+1$, where k is a natural number, whence, as we learned above, Theorem 11ª follows. □

As an application of Theorem 11ª we give a proof of the following theorem of A. Mąkowski (cf. Chapter V, § 7):

For any natural number $k \geqslant 2$ there exist infinitely many composite natural numbers n such that the relation $n \mid a^{n-k}-1$ holds for any integer a with $(a, n) = 1$.

PROOF. Let $k = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$, where $q_1 < q_2 < \dots < q_s$, be the factorization of a natural number $k \geqslant 2$ into prime factors. In view of Theorem 11^a there exist infinitely many prime numbers $p > k$ each of the form $(q_1-1)(q_2-1)\dots(q_s-1)t+1$, where t is a natural number. We are going to prove that if p is any of those numbers, then the number $n = kp$ is a composite number, whose existence the theorem asserts.

In fact, we have

$$\begin{aligned} n-k = k(p-1) &= q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}(q_1-1)(q_2-1)\dots(q_s-1)t \\ &= q_1 q_2 \dots q_s \varphi(k) t, \end{aligned}$$

whence, in virtue of the theorem of Euler and the theorem of Fermat, we infer that for $(a, n) = 1$ the number $a^{n-k}-1$ is divisible by k and p, and so it is divisible by $kp = n$. □

Another application of Theorem 11^a is this. We call a sequence $p, p+2, p+6$ whose elements are all primes a *triplet of the first category* and a sequence $p, p+4, p+6$, whose elements are all prime numbers, a *triplet of the second category.*

We prove that if from the set of primes we remove those primes which belong to triplets of the first or of the second category, then infinitely many primes still remain in the set.

In fact, as follows from Theorem 11^a, there exist infinitely many prime numbers q of the form $q = 15k+1$ where k is a natural number. Trivially, for any of the q's we have $3 \mid q+2$, $5 \mid q+4$, $3 \mid q-4$, $5 \mid q-6$. Therefore, since $q > 15$, the numbers $q+2$, $q+4$, $q-4$ and $q-6$ are composite. Hence it follows immediately that q cannot be any of the numbers which belong to any triplet of the first or of the second category. In fact, if q were any of those numbers, i.e. if either $q = p$ or $q = p+2$ or $q = p+6$ and the numbers $p, p+2, p+6$ were prime, then, in the first case, the number $p+2 = q+2$ would be composite, in the second case, the number $p+6 = q+4$ would be composite, and finally, in the third case the number $p = q-6$ would be composite. Thus we see that none of the cases is possible. Similarly, if the numbers $p, p+4, p+6$ are prime, then, if $p = q$, $p+4 = q+4$ is a composite number, if $q = p+4$, then $p+6 = q+2$ is composite, and, finally, if $q = p+6$, then $p = q-6$ is composite.

6. Proof of the existence of the primitive root of a prime number

Let p denote a given prime number. By the corollary to Theorem 9, the terms of the sequence

$$1, 2, 3, \ldots, p-1 \tag{23}$$

belong (mod p) to the exponents which are divisors of number $\varphi(p) = p-1$. For each natural divisor δ of number $p-1$ denote by $\psi(\delta)$ the number of those elements of sequence (23) which belong to exponent δ with respect to modulus p. Since each of the elements of sequence (23) is relatively prime to p, they must belong to an exponent δ which is a divisor of number $p-1$. Consequently,

$$\sum_{\delta | p-1} \psi(\delta) = p-1.$$

Since, in view of Theorem 7, $\sum\limits_{\delta|p-1} \varphi(\delta) = p-1$, we have

$$\sum_{\delta|p-1} (\varphi(\delta) - \psi(\delta)) = 0. \tag{24}$$

We are going to prove that $\psi(\delta) \leqslant \varphi(\delta)$ for $\delta \mid p-1$. Plainly this is true for $\psi(\delta) = 0$. Suppose that $\psi(\delta) > 0$, i.e. that sequence (23) contains at least one number a which belongs to exponent δ with respect to modulus p. We then have $a^\delta \equiv 1 \pmod{p}$. Consequently, number a is one of the roots of the congruence

$$x^\delta - 1 \equiv 0 \pmod{p}. \tag{25}$$

Let

$$r_1, r_2, \ldots, r_\delta \tag{26}$$

be the remainders obtained by dividing the numbers $a^k (k = 1, 2, \ldots, \delta)$ by p. Numbers (26) are different because otherwise, if $r_k = r_{k+l}$, where k, l are natural numbers and $k+l \leqslant \delta$, then $p \mid a^{k+l} - a^k = a^k(a^l - 1)$, whence, taking into account the relation $(a, p) = 1$, we infer that $p \mid a^l - 1$, i.e. $a^l \equiv 1 \pmod{p}$, which is impossible because a belongs to exponent δ with respect to modulus p, and l is a natural number less than δ (in fact, $k+l \leqslant \delta$ and $k \geqslant 1$ give $l < \delta$). According to the definition of numbers (26), for $k = 1, 2, \ldots, \delta$ the relation $r_k \equiv a^k \pmod{p}$ holds. Hence, in virtue of $a^\delta \equiv 1 \pmod{p}$, we have $r_k^\delta \equiv (a^\delta)^k \equiv 1 \pmod{p}$, which proves that numbers (26) are roots of congruence (25). Congruence (25), however, is of δth degree and satisfies the conditions of Lagrange's theorem

(Theorem 13, § 8, Chapter V), so it cannot have any other solution than those given by the δ numbers (26).

On the other hand, any of the numbers x that belongs to exponent δ with respect to modulus p satisfies congruence (25); so it is one of the numbers (26). Our aim is to find numbers r_k which belong to the exponent δ with respect to the modulus p. We prove that they are precisely the numbers r_k for which $(k, \delta) = 1$.

Suppose that $(k, \delta) = 1$. Then the number r_k, as a root of congruence (25), belongs to the exponent $\delta' \leqslant \delta$ with respect to the modulus p. Therefore $r_k^{\delta'} \equiv 1 \pmod p$. But $r_k \equiv a^k \pmod p$, whence $a^{k\delta'} \equiv 1 \pmod p$. We see that number $k\delta'$ is one of the roots of the congruence $a^x \equiv 1 \pmod p$. Hence, by Theorem 9, $\delta \mid k\delta'$, which in virtue of the assumption $(k, \delta) = 1$, gives $\delta \mid \delta'$, and this, by $\delta' \leqslant \delta$, proves that $\delta' = \delta$. Thus we see that if $(k, \delta) = 1$, then r_k belongs to the exponent δ with respect to the modulus p.

Now, suppose the opposite, i.e. that $(k, \delta) = d > 1$. Let $k = k_1 d$, $\delta = \delta_1 d$, where $\delta_1 < \delta$. Then $k\delta_1 = k_1 d\delta_1 = k_1 \delta$.

Consequently,

$$r_k^{\delta_1} \equiv a^{k\delta_1} \equiv a^{k_1\delta} \equiv (a^\delta)^{k_1} \equiv 1 \pmod p.$$

This shows that $r_k^{\delta_1} \equiv 1 \pmod p$, where $\delta_1 < \delta$, and so the number r_k cannot belong to the exponent δ with respect to the modulus p. We have thus proved that the condition $(k, \delta) = 1$ is both necessary and sufficient in order that number r_k should belong to the exponent δ with respect to the modulus p. In other words, it has turned out that numbers r_k of sequence (26) which belong to the exponent δ with respect to the modulus p are precisely those whose indices k are relatively prime to δ. The number of them is clearly $\varphi(\delta)$. Thus if (for a given natural divisor δ of number $p-1$) $\psi(\delta) > 0$, then $\psi(\delta) = \varphi(\delta)$. It follows that all the summands of (24) are non-negative, which, in virtue of the fact that the sum is equal to zero, proves that each of the summands must be equal to zero. Hence, trivially, $\psi(\delta) = \varphi(\delta)$ for $\delta \mid p-1$.

We have thus proved the following

THEOREM 12. *Let p be a prime and δ a natural divisor of the number $p-1$. Then there are precisely $\varphi(\delta)$ different numbers of the sequence $1, 2, \ldots, p-1$ that belong to the exponent δ with respect to the modulus p.*

As an important special case, for $\delta = p-1$, we obtain

COROLLARY. *Every prime number p has $\varphi(p-1)$ primitive roots among the terms of the sequence* $1, 2, \ldots, p-1$.

A glance at the proof of the theorem shows that if g is a primitive root of a prime p, then all the primitive roots of p that belong to sequence (23) are to be found among the remainders yielded by the division by p of those terms of the sequence

$$g, g^2, g^3, \ldots, g^{p-1}$$

whose exponents are relatively prime to $p-1$.

Denote by $\gamma(p)$ the least primitive root of a prime p. The following table shows the values of the function $\gamma(p)$ for odd primes $p < 100$:

p	3	5	7	11	13	17	19	23	29	31	37	41
$\gamma(p)$	2	2	3	2	2	3	2	5	2	3	2	6

p	43	47	53	59	61	67	71	73	79	83	89	97
$\gamma(p)$	3	5	2	2	2	2	7	5	3	2	3	5

It has been proved that $\overline{\lim}\,\gamma(p) = \infty$ (Pillai [7]) and even that, for infinitely many p, $\gamma(p) > c\log p$ (cf. Turán [1]). On the other hand, we do not know whether there exist infinitely many primes for which number 2 is a primitive root. E. Artin has conjectured that every integer $g \neq -1$ which is not a square is a primitive root of infinitely many primes (cf. Hasse [1], p. 68). This can be deduced from the Conjecture H (cf. Schinzel and Sierpiński [3], pp. 199–201).

The table presented above shows that $\gamma(p) \leqslant 7$ for any prime $p < 100$. For $p < 191$ we also have $\gamma(p) \leqslant 7$, but $\gamma(191) = 19$. If $p < 409$, then $\gamma(p) \leqslant 19$, but $\gamma(409) = 21$. For primes $p < 3361$ we have $\gamma(p) \leqslant 21$, but $\gamma(3361) = 22$. For $p < 5711$ we have $\gamma(p) \leqslant 22$, but $\gamma(5711) = 29$. If p is a prime < 5881, then $\gamma(p) \leqslant 29$, but $\gamma(5881) = 31$ (cf. Wertheim [1], pp. 406–409).

If g is a primitive root of a prime p, then the numbers $g^0, g^1, g^2, \ldots, g^{p-2}$ divided by p leave different remainders, each of them, in addition, being different from zero. Consequently, the number of the remainders is equal to the number of the numbers $g^0, g^1, g^2, \ldots, g^{p-2}$, i.e. it is equal to $p-1$. Therefore, for any number $x = g^0, g^1, \ldots, g^{p-2}$, there exists a number y of the sequence $0, 1, 2, \ldots, p-2$ such that $g^y \equiv x \pmod{p}$.

Now we are going to establish all the natural numbers $m > 1$ which have primitive roots. The situation is described by the following theorem:

A natural number $m > 1$ has primitive roots if and only if it is one of the numbers

$$2, 4, p^\alpha, 2p^\alpha$$

where p is an odd prime and α a natural number. The number of primitive roots of any number m of this form is $\varphi(\varphi(m))$ (cf. Sierpiński [12], p. 193).

It has been verified by Litver and Yudina [1] that for all the primes $p \leqslant 10^6$ except $p = 40487$ $\gamma(p)$ is a primitive root of p^α for all α.

As an application of the theorem on the existence of primitive roots of odd prime numbers, we shall find all the natural numbers m for which the congruences $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply the congruence $a^c \equiv b^d \pmod{m}$ for any positive integers a, b, c, d.

For simplicity, we call the above-mentioned property of number m property P. Suppose that a natural number m has property P. Let a denote a given integer. In virtue of the obvious relations $m \mid a-a$ and $m \mid (m+1)-1$ we then have $m \mid a^{m+1}-a$, i.e. $m \mid a(a^m-1)$. On the other hand, suppose that number m is such that for any integer a we have $m \mid a(a^m-1)$. Let a, b, c, d be integers such that $m \mid a-b$ and $m \mid c-d$. If $c = d$, then, by $m \mid a-b$, we have $m \mid a^c-b^d$. Suppose that $c \neq d$. Interchanging, if necessary, the roles of c and d, we assume that $c > d$. Then, since $m \mid c-d$, $c = d+mk$, where k is a natural number. We then have $a \mid a^d$ and $a^m-1 \mid a^{mk}-1$. Moreover, it follows from $m \mid a(a^m-1)$ that $m \mid a^d(a^{mk}-1) = a^c-a^d$. But, in virtue of $m \mid a-b$, we have $m \mid a^d-b^d$, which, by the formula $m \mid a^c-a^d$ gives $m \mid a^c-b^d$. We see that number m has property P. We have thus proved that a necessary and sufficient condition for a number m to have property P is that for any integer a, $m \mid a(a^m-1)$.

Now, our aim is to find all the numbers m that have property P. Trivially, numbers 1 and 2 have property P. Suppose that m is a natural number > 2. If m were divisible by a square of a prime number p, then, for $a = p$, we would have $p^2 \mid p(p^m-1)$, which is impossible because $(p, p^m-1) = 1$. Consequently, number m must be a product of different prime factors; being greater than 2, the product must contain a prime odd factor p. Let g denote a primitive root of the prime p. Since $p \mid m \mid g(g^m-1)$ and $(p, g) = 1$, we find that $p \mid g^m-1$. But since g belongs to the exponent $p-1$ with respect to modulus p, we have $p-1 \mid m$. Therefore number m is even and is the product of at least two different prime factors 2, and p. If m is the product of precisely those two different prime factors, then $m = 2p$. Since $p-1 \mid m$ and $(p-1, p) = 1$, we have $p-1 \mid 2$; so, in view of $p \geqslant 3$ (since p is an odd prime), we conclude that $p = 3$ and consequently $m = 2 \cdot 3 = 6$. Number 6 indeed has property P because, as we know, for any integer a we have $6 \mid (a-1)a(a+1) = a(a^2-1)$ and $a^2-1 \mid a^6-1$, whence $6 \mid a(a^6-1)$.

We now suppose that m is a product of three (necessarily different) prime factors, i.e. $m = 2p_1p_2$, where $2 < p_1 < p_2$. As we know, $p_1-1 \mid m$ that is $p_1-1 \mid 2p_1p_2$. But $p_1-1 > 1$ (since $p_1 > 2$) and also $p_1-1 < p_1 < p_2$. The prime p_2 cannot be divisible by p_1-1 and therefore $p_1-1 \mid 2p_1$, whence, in analogy to the previous case, we infer that $p_1 = 3$, and so $m = 6p_2$. In virtue of the relations $p_2-1 \mid m = 6p_2$ and $(p_2-1, p_2) = 1$, one has $p_2-1 \mid 6$, which, by the fact that $p_2 > p_1$ i.e. that $p_2 > 3$ and so $p_2-1 > 2$, gives either $p_2-1 = 3$ or $p_2-1 = 6$. But $p_2-1 = 3$ is impossible because p_2 is a prime, so $p_2-1 = 6$ is valid, whence $p_2 = 7$ and consequently $m = 2 \cdot 3 \cdot 7 = 42$. As can easily be verified, number 42 indeed has property P. In fact, as is known, $6 \mid a(a^6-1)$ holds for any integer a, whence *a fortiori* $6 \mid a(a^{42}-1)$. If a is not divisible by 7, then, in virtue of the theorem of Fermat, $7 \mid a^6-1$, whence again $7 \mid a(a^{42}-1)$. Thus we see that for any integer a the relations $6 \mid a(a^{42}-1)$ and $7 \mid a(a^{42}-1)$ simultaneously hold, which, by $(6, 7) = 1$, gives $42 \mid a(a^{42}-1)$, and this proves that number 42 has property P.

Further we suppose that m is a product of four prime factors. That is that $m = 2p_1 p_2 p_3$, where $2 < p_1 < p_2 < p_3$. Then, as in the above argument, we infer that $p_1-1 \mid 2$, whence $p_1 = 3$; similarly, $p_2-1 \mid 2p_1 = 6$, whence $p_2 = 7$; and finally $p_3-1 \mid$ $\mid 2p_1 p_2 = 42$. Therefore, since $p_3 > p_2 = 7$, it must be true that $p_3-1 = 7, 14, 21$ or 42, which, in virtue of the fact that p_3 is a prime, implies $p_3-1 = 42$, i.e. $p_3 = 43$, whence m $= 1806$. It is easy to see that number 1806 has property P because, as we have just proved, $42 \mid a(a^{42}-1)$ for any integer a, whence *a fortiori* $42 \mid a(a^{1806}-1)$. If a is divisible by 43, then we have $43 \mid a(a^{1806}-1)$; if a is not divisible by 43, this relation is a simple consequence of the theorem of Fermat, because then $43 \mid a^{42}-1$, whence *a fortiori* $43 \mid a^{1806}-1$. The relations $42 \mid a(a^{1806}-1)$ and $43 \mid a(a^{1806}-1)$, valid for any integer a, give by $(42, 43) = 1$ and $1806 = 42 \cdot 43$ the required relation $1806 \mid a(a^{1806}-1)$, which proves that number 1806 has property P.

Finally, we suppose that m is a product of more than four prime factors. That is $m = 2p_1 p_2 \ldots p_k$, where $k \geqslant 4, 2 < p_1 < p_2 < \ldots < p_k$. As we have seen above, $p_1 = 3$, $p_2 = 7$, $p_3 = 43$. Further, $p_4-1 \mid m$, whence, as can easily be found, $p_4-1 \mid 2p_1 p_2 p_3$, i.e. $p_4-1 \mid 1806$. On the other hand, $p_4-1 > p_3-1 = 42$, and, moreover, p_4-1 is even. Even divisors of the number $1806 = 2 \cdot 3 \cdot 7 \cdot 43$ which are greater than 42 are the numbers 86, 258, 602, 1806. Therefore p_4 must be one of the numbers 87, 259, 603, or 1807, but none of them is prime. We have $87 = 3 \cdot 29$, $259 = 7 \cdot 37$, $603 = 3^2 \cdot 67$, $1807 = 13 \cdot 139$. Thus we see that the assumption that a number m is a product of more than four prime factors leads to a contradiction.

We have thus proved the theorem of J. Dyer Bennet [1], stating that *the numbers* 1, 2, 6, 42, 1806 *are the only ones which have property* P. Consequently, they are the only moduli m for which the congruences $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply a^c $\equiv b^d \pmod{m}$ for any positive integers a, b, c, d.

As is easy to notice, numbers m which have property P are precisely those squarefree integers m for which $\lambda(m) \mid m$, where $\lambda(m)$ is the minimum universal exponent with respect to the modulus m (cf. § 4).

EXERCISE. Prove that number 2 is not a primitive root of any prime number of the form $2^{2^n}+1$, where n is a natural number > 1.

PROOF. If p is a prime number and $p = 2^{2^n}+1$, then $2^{2^{n+1}} \equiv 1 \pmod{p}$. But $p-1$ $= 2^{2^n} > 2^{n+1}$ for $n > 1$ because, as can easily be proved by induction, $2^n > n+1$ for n $= 2, 3, \ldots$ Consequently number 2 belongs to an exponent $< p-1$ with respect to the modulus p and is not a primitive root of p. □

7. An *n*th power residue for a prime modulus *p*.

If p is a prime, n a natural number > 1, then an integer a is called an *n-th power residue for the modulus p* whenever there exists an integer x such that $x^n \equiv c \pmod{p}$. Clearly, the number 0 is an nth power residue for the modulus p for any prime p and integer n. Therefore we generally assume that any nth power residue we are concerned with is different from zero.

From the purely theoretical point of view, there exists a method for establishing whether a given natural number $a \neq 0$ is an nth power residue for a given modulus p. In fact, it is sufficient to check whether there exists a number x in the sequence $1, 2, \ldots, p-1$ which satisfies the congruence $x^n \equiv a \pmod{p}$.

In this connection, we have the following

THEOREM 13 (Euler). *An integer a which is not divisible by a prime p is an n-th power residue for the prime modulus p if and only if the relation*

$$a^{(p-1)/d} \equiv 1 \pmod{p} \quad \text{with} \quad d = (p-1, n) \tag{27}$$

holds.

PROOF. Suppose that an integer a, which is not divisible by a prime p, is an nth power residue for the modulus p. Then there exists an integer x, of course not divisible by p, such that $a \equiv x^n \pmod{p}$. Hence

$$a^{(p-1)/d} \equiv (x^n)^{(p-1)/d} \equiv (x^{p-1})^{n/d}. \tag{28}$$

Since $d \mid n$, and, by the theorem of Fermat, $x^{p-1} \equiv 1 \pmod{p}$, from (28) we infer the truth of (27). Thus we see that the condition is necessary.

Suppose now that formula (27) holds. Let g be a primitive root of p. As we learned in § 6, there exists an integer h such that $0 \leqslant h \leqslant p-2$ and $a \equiv g^h \pmod{p}$ which, invirtue of (27), proves that $g^{h(p-1)/d} \equiv 1 \pmod{p}$. Since g is a primitive root for the prime p, the last relation implies that $p-1 \mid \dfrac{h(p-1)}{d}$, which gives $d \mid h$ and so $h = kd$, where k is a non-negative integer. According to the definition, $d = (p-1, n)$, which, by Theorem 16 from Chapter I, proves that there exist two natural numbers u, v such that $d = nu-(p-1)v$, whence $kd = knu-k(p-1)v$. But, in virtue of the theorem of Fermat, $g^{k(p-1)v} \equiv 1 \pmod{p}$. Hence, using the relations $a \equiv g^h \equiv g^{kd} \pmod{p}$, we find $a \equiv ag^{k(p-1)v} \equiv g^{kd+k(p-1)v} \equiv g^{knu} \equiv (g^{ku})^n \pmod{p}$, which proves that a is an nth power residue for the prime p. This proves the sufficiency of the condition. Theorem 13 is thus proved. □

If a is an nth power residue for a modulus p, then, clearly, every number that is congruent to $a \pmod{p}$ is also an nth power residue for the modulus p. Therefore the number of nth power residues for a given modulus p is understood as the number of mutually non-congruent (mod p) nth power residues for the modulus p.

THEOREM 14. *If p is a prime, n a natural number and $d = (n, p-1)$, then the number of different n-th power residues for the modulus p (number 0 included) is $(p-1)/d+1$.*

PROOF. Let g be a primitive root for the modulus p. Let $d = (p-1, n)$, $n = dm$, $p-1 = ds$, where m, s are natural numbers and $(m, s) = 1$. Let k, l be any two numbers of the sequence $1, 2, \ldots, s$ such that $k > l$. If $g^{kn} \equiv g^{ln} \pmod{p}$, then $p \mid g^{kn} - g^{ln} = g^{ln}(g^{(k-l)n} - 1)$, so, by $(p, g) = 1$, $g^{(k-l)n} \equiv 1 \pmod{p}$. Hence, since g is a primitive root for the prime p, $p-1 \mid (k-l)\,n$, which, in virtue of the relations $n = dm$, $p-1 = ds$, gives $s \mid (k-l)\,m$; so, since $(m, s) = 1, s \mid k-l$, which is impossible because k and l are two different numbers of the sequence $1, 2, \ldots, s$. Thus we conclude that the numbers $g^n, g^{2n}, \ldots, g^{sn}$ divided by p yield different remainders. Moreover, each of these numbers is an nth power residue for the modulus p (since the congruence $x^n \equiv g^{kn} \pmod{p}$ has an obvious solution $x = g^k$). Therefore there are at least s different nth power residues for the modulus p, each of them different from zero.

Now let a denote an arbitrary nth power residue for the modulus p different from zero. Then there exists an integer x (clearly not divisible by p) such that $x^n \equiv a \pmod{p}$. As we have learned, in the sequence $0, 1, \ldots, p-2$ there exists a number y such that $x \equiv g^y \pmod{p}$, whence $a \equiv g^{ny} \pmod{p}$. Let r denote the remainder obtained by dividing y by x. We then have $y = ks+r$, where k is a non-negative integer and $0 \leqslant r < s$. Hence $ny = nks+nr$. But, since $n = dm$, $p-1 = ds$, we have $ns = (p-1)\,m$. Consequently, $ny = k(p-1)\,m+nr$, whence $a \equiv g^{ny} \equiv g^{nr} \pmod{p}$, and this shows that there are no nth power residues for the modulus p different from zero other than $1, g^n, g^{2n}, \ldots, g^{(s-1)n}$. Since $sn = (p-1)\,m$, residue 1 can be replaced by the residue g^{sn}. We have thus proved that for a given prime modulus p there exist precisely $\dfrac{p-1}{(n, p-1)}+1$ different nth power residues. □

As an immediate corollary to Theorem 14 we have the following proposition: *in order that for a given natural number n every integer be an n-th power residue for a given prime modulus p it is necessary and sufficient that n be relatively prime to $p-1$.*

Accordingly, in the case of $n = 3$, in order that every integer be a third power residue for a prime modulus p it is necessary and sufficient that p should not be of the form $3k+1$, where k is a natural number, i.e. that it should be either one of the numbers 2, 3 or of the form $3k+2$, where k is a natural number.

It is easy to prove that there are infinitely many primes of the form $3k+2$. In fact, let n denote an arbitrary natural number and let $N = 6n!-1$. Clearly, N is a natural number > 1. It is easy to see that any divisor of the number N is of the form $6k+1$ or $6k-1$. Not all prime divisors of N are of the form $6k+1$ since, if they were, their product would be of this form, which is trivially untrue since N is not of this form. Consequently, number N has at least one prime divisor $p = 6k-1$, where k is a natural number. The relation $p \mid N = 6n!-1$ implies that $p > n$. This, since n is arbitrary, shows that there exist arbitrarily large primes of the form $6k-1 = 3(2(k-1)+1)+2$, as was to be proved.

It can be proved that if n is a prime and m a natural number > 1, then in order that every integer be an nth power residue for the modulus m it is necessary and sufficient that m be a product of different primes, none of the form $nk+1$ (where k is a natural number) (cf. Sierpiński [9]).

EXERCISE. Prove that if p is a prime, n a natural number and $d = (p-1, n)$, then the nth power residue for the prime p coincides with the dth power residue for the prime p.

PROOF. By $d = (p-1, n)$ we have $d \mid p-1$, so $d = (p-1, d)$ and consequently, by theorem 13, a necessary and sufficient condition for an integer a, not divisible by p, to be an nth power residue for the modulus p is the same as that for a to be a dth power residue for the modulus p. Therefore the sets of nth power residues and dth power residues for the modulus p coincide.

In particular, it follows that if p is a prime of the form $4k+3$, where $k = 0, 1, 2, \ldots$, then (since $2 = (p-1, 4)$), the quadratic residues for the modulus p coincide with the 4th power residues for the modulus p. ☐

8. Indices, their properties and applications

In § 4 we defined a primitive root of a natural number m as an integer g which belongs to the exponent $\varphi(m)$ with respect to the modulus m. It follows that, as we know, the numbers $g^0, g^1, \ldots, g^{\varphi(m)-1}$ are all incongruent (mod m). Since the number of them is $\varphi(m)$, this being equal to the number of the numbers relatively prime to m which appear in the sequence $1, 2, \ldots, m$, then for any integer x relatively prime to m there exists precisely one number y in the sequence $0, 1, 2, \ldots, \varphi(m)-1$ such that $g^y \equiv x \pmod{m}$. We say that y is the *index* of x relative to the primitive root g. It is denoted by $\mathrm{ind}_g\, x$, or, if no confusion is likely to ensue, by $\mathrm{ind}\, x$. We call g the *base* of the index.

Now we fix a natural number $m > 1$ which admits a primitive root g and consider the indices $\mathrm{ind}\, x$ of integers x relatively prime to the number m. We prove the following properties of indices:

I. *The indices of integers which are congruent* (mod m) *are equal.* (Needless to say, the primitive roots are assumed to be equal and the integers to be relatively prime to m.)

In fact, if $a \equiv b \pmod{m}$ and, $g^{\mathrm{ind} a} \equiv a \pmod{m}$, then $g^{\mathrm{ind} a} \equiv b \pmod{m}$. But, as we know, since $(b, m) = 1$, the congruence $g^x \equiv b \pmod{m}$ has precisely one root among the numbers $0, 1, \ldots, \varphi(m)-1$, and this is $\mathrm{ind}\, b$; we conclude that $\mathrm{ind}\, a = \mathrm{ind}\, b$.

Therefore in the tables of indices the values of $\mathrm{ind}\, x$ are given only for natural numbers x less than the modulus (and relatively prime to it).

II. *The index of the product is congruent* (mod $\varphi(m)$) *to the sum of the indices of the factors*, i.e.

$$\mathrm{ind}\,(ab) \equiv \mathrm{ind}\, a + \mathrm{ind}\, b \pmod{\varphi(m)}. \tag{29}$$

In fact, according to the definition of indices, we have $g^{\mathrm{ind} a} \equiv a \pmod{m}$, $g^{\mathrm{ind} b} \equiv b \pmod{m}$ (whenever a and b are relatively prime to m). Hence, multiplying the last two congruences, we obtain

$$g^{\mathrm{ind} a + \mathrm{ind} b} \equiv ab \pmod{m}.$$

But since $g^{\mathrm{ind}(ab)} \equiv ab \pmod{m}$, we infer that

$$g^{\mathrm{ind}(ab)} \equiv g^{\mathrm{ind} a + \mathrm{ind} b} \pmod{m}. \tag{30}$$

Suppose that for any non-negative integers μ, ν the congruence $g^\mu \equiv g^\nu \pmod{m}$ holds. If $\mu \geqslant \nu$, then $m \mid g^\nu(g^{\mu-\nu}-1)$, which, in virtue of the fact that $(g, m) = 1$, implies $g^{\mu-\nu} = 1 \pmod{m}$. Number g, as a primitive root of m, belongs to the exponent $\varphi(m)$ with respect to the modulus m. Hence, by Theorem 9, it follows that $\varphi(m) \mid \mu-\nu$.

The last relation remains true also in the case where $\mu \leqslant \nu$. Thus, from (30) congruence (29) follows.

The property just proved is easily generalized to any finite number of factors. Hence

III. *The index of the n-th power (n being a natural number) is congruent* (mod $\varphi(m)$) *to the product of n multiplied by the index of the base. We have*

$$\mathrm{ind}\, a^n \equiv n\, \mathrm{ind}\, a \pmod{\varphi(m)}.$$

Now we are going to establish the relation between indices taken with respect to different primitive roots of a fixed number m. According to the definition of the index, we have

$$a \equiv g^{\mathrm{ind}_g a} (\mathrm{mod}\, m).$$

Hence, using properties I and III, we obtain

$$\mathrm{ind}_\gamma a \equiv \mathrm{ind}_g a \cdot \mathrm{ind}_\gamma g\, (\mathrm{mod}\ \varphi(m)),$$

where γ is a primitive root of m. Hence

In order to change the base of indices it is sufficient to multiply each of them by a fixed number (namely by the index of the former base relative to the new base) and to find the residues for the modulus $\varphi(m)$ of the products.

THEOREM 15. *In order that a number a, which is not divisible by p, be a quadratic residue for an odd prime p, it is necessary and sufficient that* ind a *be even.*

PROOF. Suppose that $\mathrm{ind}_g a = 2k$, where k is a non-negative integer. We have $g^{2k} \equiv a\, (\mathrm{mod}\, p)$, which shows that the congruence $x^2 \equiv a\, (\mathrm{mod}\, p)$ has a root $x = g^k$. Therefore number a is a quadratic residue for the modulus p.

In the sequence $1, 2, ..., p-1$ there are, of course, $\frac{1}{2}(p-1)$ numbers whose indices are even. (The proof follows from the remark that the indices of the numbers of the sequence coincide with the numbers $0, 1, 2, ..., p-2$ in a certain order; among $0, 1, 2, ..., p-2$, however, there are precisely $\frac{1}{2}(p-1)$ even numbers.) Each of these numbers is then a quadratic residue for the prime p. But, by Theorem 14 (with $d = (2, p-1) = 2$), there are only $\frac{1}{2}(p-1)$ quadratic residues in the sequence $1, 2, ..., p-1$. From this we infer that none of the numbers with odd indices can be a quadratic residue for the prime p. The theorem is thus proved. □

It is an immediate consequence of Theorem 15 that none of the primitive roots of an odd prime p can be a quadratic residue to p.

We note that an analogous theorem for an nth power residue with n greater than 2 is not true. For example, among the indices relative to the modulus 5 there are only two, 0 and 3, divisible by 3, and each of the numbers 1, 2, 3, 4 is a 3rd power residue to 5. (In fact, $1 \equiv 1^3 (\mathrm{mod}\ 5)$, $2 \equiv 3^3 (\mathrm{mod}\ 5)$, $3 \equiv 2^3 (\mathrm{mod}\ 5)$, $4 \equiv 4^3 (\mathrm{mod}\ 5)$). For the modulus 7 the numbers $1 \equiv 1^4 (\mathrm{mod}\ 7)$, $2 \equiv 2^4 (\mathrm{mod}\ 7)$, $4 \equiv 3^4 (\mathrm{mod}\ 7)$ are 4th power residues; among the indices relative to the modulus 7, however, there are only two, 0 and 4, divisible by 4.

Indices are applied in solving congruences.

Let p be a prime, and a, b numbers not divisible by p. Consider the congruence

$$ax \equiv b \pmod{p}.$$

By properties I and II

$$\operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1},$$

whence

$$\operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}.$$

The number $\operatorname{ind} x$ is thus the remainder left by the difference $\operatorname{ind} b - \operatorname{ind} a$ divided by number $p-1$. Thus, knowing the value of $\operatorname{ind} x$, we find x by $x \equiv g^{\operatorname{ind} x} \pmod{p}$. Of course, to aply this method in practice one should have the tables of indices $(\operatorname{mod} p)$.

Now let a be an integer which is not divisible by p, and n a natural exponent. Consider the congruence

$$x^n \equiv a \pmod{p}.$$

By properties I and III it follows that the congruence is equivalent to the congruence

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}.$$

Thus the problem of solving binomial congruences reduces to that of solving linear congruences.

Consider an exponential congruence

$$a^x \equiv b \pmod{p},$$

where a, b are integers not divisible by the prime p. The congruence is equivalent to the linear congruence

$$x \operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}.$$

EXAMPLES. We are going to tabulate the indices (mod 13). Accordingly, first we have to establish a primitive root of 13. We begin with the least possible number 2.

We find the residue (mod 13) of the consecutive powers of number 2. Clearly, it is necessary to calculate number 2^n for every natural exponent n; for, if r_k is the remainder obtained by dividing 2^k by 13, then the remainder yielded by 2^{k+1} divided by 13 is equal to the remainder of $2r_k$.

In this way we find $2 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 3$, $2^5 \equiv 6$, $2^6 \equiv 12$, $2^7 \equiv 11$, $2^8 \equiv 9$, $2^9 \equiv 5$, $2^{10} \equiv 10$, $2^{11} \equiv 7$, $2^{12} \equiv 1 \pmod{13}$.

This proves that 2 is a primitive root of 13. We tabulate the numbers x according to their indices $\operatorname{ind}_2 x \equiv k$ (where $k = 0, 1, \ldots, 11$) as follows:

$\operatorname{ind}_2 x$	0	1	2	3	4	5	6	7	8	9	10	11
x	1	2	4	8	3	6	12	11	9	5	10	7

By the use of this table we can tabulate the indices according to the numbers $x = 1, 2, \ldots, 12$ as follows:

x	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 x$	0	1	4	2	9	5	11	3	8	10	7	6

Given a congruence

$$6x \equiv 5 \pmod{13}.$$

We have $\operatorname{ind} 6 + \operatorname{ind} x \equiv \operatorname{ind} 5 \pmod{12}$, whence $\operatorname{ind} x \equiv \operatorname{ind} 5 - \operatorname{ind} 6 \pmod{12}$. As we check in the second table, $\operatorname{ind} 5 = 9$ and $\operatorname{ind} 6 = 5$, thus we find $\operatorname{ind} x \equiv 9 - 5 \equiv 4 \pmod{12}$, and so $\operatorname{ind} x = 4$ and, using the first table, we infer that $x = 3$.

Consider the congruence

$$x^8 \equiv 3 \pmod{13}.$$

We have $8 \operatorname{ind} x \equiv \operatorname{ind} 3 \pmod{12}$. On the other hand, by the tables presented above, we see that $\operatorname{ind} 3 = 4$, whence, putting $\operatorname{ind} x = y$, we obtain the congruence $8y \equiv 4 \pmod{12}$. This is equivalent to the relation $12 \mid 8y - 4$, which, in turn, is equivalent to $3 \mid 2y - 1$, i.e. to the congruence $2y \equiv 1 \pmod 3$. Hence $4y \equiv 2 \pmod 3$. But, since $4 \equiv 1 \pmod 3$, $y \equiv 2 \pmod 3$ and therefore $y = 2 + 3k$, where k is an integer. Numbers of this form that belong to the sequence $0, 1, 2, \ldots, 11$ are the numbers 2, 5, 8 and 11. Consequently, they are the values of $y = \operatorname{ind} x$. Using the first table for x we find the values 4, 6, 9 and 7. Thus we see that the congruence has precisely four solutions, 4, 6, 7, 9.

Finally, consider the congruence

$$6^x \equiv 7 \pmod{13}.$$

We then have $x \operatorname{ind} 6 \equiv \operatorname{ind} 7 \pmod{12}$. As we check in the second table, $\operatorname{ind} 6 = 5$, $\operatorname{ind} 7 = 11$. Thus the congruence turns into the congruence $5x \equiv 11 \pmod{12}$, which is satisfied only for $x = 7$, provided the x's are taken out of the sequence $0, 1, \ldots, 11$. Consequently, all the solutions of the congruence are numbers of the form $7+12k$, where $k = 0, 1, 2, \ldots$

EXERCISES. **1.** Prove that for any odd prime modulus p relative to any primitive root of p, the equalities $\operatorname{ind}(-1) = \operatorname{ind}(p-1) = \frac{1}{2}(p-1)$ hold.

PROOF. In virtue of the theorem of Fermat, for any primitive root g of an odd prime p the relation $p \mid g^{p-1}-1 = (g^{\frac{1}{2}(p-1)}-1)(g^{\frac{1}{2}(p-1)}+1)$ holds. But since $p \mid g^{\frac{1}{2}(p-1)}-1$ is impossible (because g is a primitive root of p), $p \mid g^{\frac{1}{2}(p-1)}+1$ is valid, i.e. $g^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$, which shows that $\operatorname{ind}(-1) = \frac{1}{2}(p-1)$. □

2. Prove that a necessary and sufficient condition for an integer g relatively prime to an odd prime p to be a primitive root of p is the validity of the relation $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ for any prime divisor q of the number $p-1$.

PROOF. If for a prime q the relations $q \mid p-1$ and $g^{(p-1)/q} = 1 \pmod{p}$ hold, then q belongs to an exponent $\leqslant (p-1)/q < p-1$ and, consequently, g is not a primitive root of p. Thus the condition is necessary.

On the other hand, suppose that an integer g relatively prime to p is not a primitive root of p. Then the exponent δ to which g belongs with respect to modulus p is $< p-1$. As we know, δ must be a divisor of number $p=1$, whence number $(p-1)/\delta$ is a natural number > 1, and so it has a prime divisor q. We then have $q \mid (p-1)/\delta$, whence $\delta \mid (p-1)/q$ and, since $p \mid g^{\delta}-1$ (because g belongs to the exponent δ with respect to the modulus p), then *a fortiori* $p \mid g^{(p-1)/q}-1$, i.e. $g^{(p-1)/q} = 1 \pmod{p}$. The condition is thus sufficient. □

CHAPTER VII

REPRESENTATION OF NUMBERS BY DECIMALS IN A GIVEN SCALE

1. Representation of natural numbers by decimals in a given scale

Let g be a given natural number > 1. We say that a *natural number N is expressed as a decimal in the scale of g* if

$$N = c_m g^m + c_{m-1} g^{m-1} + \dots + c_1 g + c_0, \tag{1}$$

where m is an integer $\geqslant 0$ and c_n $(n = 0, 1, 2, \dots, m)$ are integers with the property

$$0 \leqslant c_n \leqslant g-1 \quad \text{for} \quad n = 0, 1, \dots, m \text{ and } c_m \neq 0. \tag{2}$$

If each number of the sequence

$$0, 1, 2, \dots, g-1 \tag{3}$$

is denoted by a special symbol, the symbols are called the *digits* and formula (1) can be rewritten in the form

$$N = (\gamma_m \gamma_{m-1} \cdots \gamma_1 \gamma_0)_g,$$

where γ_n is the digit which denotes the number c_n.

If $g \leqslant 10$, the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 are taken as the symbols to denote the numbers of (3). For example,

$N = (10010)_2$ means $N = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 = 18$,
$N = (5603)_7$ means $N = 5 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 3 = 2012$.

THEOREM 1. *Any natural number may be uniquely expressed as a decimal in the scale of g (g being a natural number > 1), i.e. it can be rewritten in form (1), where the numbers c_n $(n = 0, 1, \dots, m)$ are integers which satisfy inequalities* (2).

PROOF. Suppose that a natural number N can be represented in form (1), where c_n $(n = 0, 1, \dots, m)$ are integers satisfying conditions (2).

Let n denote one of the numbers $0, 1, 2, \ldots, m-1$. In virtue of (1) we have

$$(4)\quad \frac{N}{g^n} = c_m g^{m-n} + c_{m-1} g^{m-n-1} + \ldots c_n + \frac{c_{n-1}}{g} + \frac{c_{n-2}}{g^2} + \ldots + \frac{c_0}{g^n}.$$

But in view of (2),

$$0 \leqslant \frac{c_{n-1}}{g} + \frac{c_{n-2}}{g^2} + \ldots + \frac{c_0}{g^n} \leqslant \frac{g-1}{g} + \frac{g-1}{g^2} + \ldots + \frac{g-1}{g^n} = 1 - \frac{1}{g^n}.$$

Hence, by (4), we infer that

$$\left[\frac{N}{g^n}\right] = c_m g^{m-n} + c_{m-1} g^{m-n-1} + c_{n+1} g + c_n$$

and similarly

$$\left[\frac{N}{g^{n+1}}\right] = c_m g^{m-n-1} + c_{m-1} g^{m-n-2} + \ldots + c_{n+1}.$$

These formulae show that

$$(5)\qquad c_n = \left[\frac{N}{g^n}\right] - g\left[\frac{N}{g^{n+1}}\right] \quad \text{for any} \quad n = 0, 1, \ldots, m.$$

In virtue of (1) and (2), we also have

$$g^m \leqslant N \leqslant (g-1)(g^m + g^{m-1} + \ldots + g + 1) = g^{m+1} - 1 < g^{m+1},$$

whence $m \log g \leqslant \log N < (m+1) \log g$ and therefore

$$m \leqslant \frac{\log N}{\log g} < m+1,$$

which proves

$$(6)\qquad m = \left[\frac{\log N}{\log g}\right].$$

Formulae (6) and (5) show that if N is represented as (1) and conditions (2) are satisfied, then the numbers m and c_n ($n = 0, 1, \ldots, m$) are uniquely defined by number N. This proves that for a given natural number N (with a fixed natural number $g > 1$) there is at most one representation (1) such that conditions (2) are satisfied.

Therefore in order to prove the theorem it is sufficient to show that for any natural number N and a natural number $g > 1$ there is at least one representation (1) (conditions (2) being satisfied).

Let N_1 and c_0 be the quotient and the remainder yielded by the division of N by g. We then have $N = c_0+gN_1$. Replacing N by N_1 we find the quotient N_2 and the remainder c_1 from the division of N_1 by g. Continuing, we proceed similarly with N_2 in place of N_1 and so on.

It is clear that the quotients consecutively obtained, when positive, decrease because $N_{n+1} \leqslant N_n/g$. Since they are non-negative integers, for some $k \geqslant 1$ we must ultimately obtain $N_k = 0$. Let m denote the greatest index for which $N_m \neq 0$. We have the following sequence of equalities:

$$N = c_0+gN_1, \quad N_1 = c_1+gN_2, \quad \ldots, \quad N_{m-1} = c_{m-1}+gN_m,$$
$$N_m = c_m.$$

Hence we easily obtain the desired representation of N, namely $N = c_0 +c_1 g+c_2 g^2+ \ldots +c_m g^m$, where $c_m \neq 0$ because $N_m \neq 0$, and the numbers c_n $(n = 0, 1, \ldots, m)$, being remainders obtained from the division by g, satisfy condition (2). ☐

Thus we have proved Theorem 1 and, at the same time, we have found an algorithm for finding the representation of N as a decimal in the scale of g. The algorithm is the following: we divide N by g and denote the remainder by c_0 and the quotient by N_1; then we divide N_1 by g and denote the remainder by c_1 and the quotient by N_2. We proceed in this way until we obtain the quotient $N_{m+1} = 0$. This, as we have just seen, leads to a representation of N in form (1).

Since in the scale of $g = 2$ there are only two digits, 0 and 1, from Theorem 1 we deduce the following

COROLLARY. *Any natural number may be uniquely expressed as the sum of different powers (the exponents being non-negative integers) of number* 2.

For example: $100 = 2^6+2^5+2^2$, $29 = 2^4+2^3+2^2+2^0$, $M_n = 2^n-1 = 2^{n-1}+2^{n-2}+ \ldots +2+2^0$.

EXERCISES. 1. Find the decimals in the scale of 2 of the first twelve prime numbers.
ANSWER: 10, 11, 101, 111, 1011, 1101, 10001, 10011, 10111, 11101, 11111, 100101.

2. Prove that for every natural number m there exists a prime whose representation as a decimal in the scale of 2 is such that the last digit is 1 and the preceding m digits are equal to zero.

PROOF. By Theorem 11 of Chapter VI, for a natural number m there exist a prime p of the form $2^{m+1}k+1$, where k is a natural number. In the representation of this number as a decimals in the scale of 2, m of the last $m+1$ digits are 0 and one, at the very end, is equal to unity. ☐

REMARK. It is known that there are prime numbers whose digits in the scale of 2 are all 1. There are 30 known numbers of this kind; the greatest of them has 216091 digits (each equal to 1) in the scale of 2. We do not know whether there exist infinitely many primes of this kind. (Clearly, they coincide with the primes of the form 2^n-1.) There are known primes whose decimals in the scale of 2 consist of digits all equal to zero with the exception of the first and the last digits. For example: 11, 101, 10001, 100000001 and 10000000000000001. These are all the known primes of this form, we do not know whether there exist any other such prime. They are the primes of Fermat of the form $2^{2^n}+1$.

3. Prove that for any natural number $s > 1$ there exist at least two primes which, presented as decimals in the scale of 2, have precisely s digits.

PROOF. For $s = 2$ and $s = 3$ the result follows from exercise 1. If $s \geqslant 4$, then $2^{s-1} > 5$ and, by Theorem 7 of Chapter III, it follows that between 2^{s-1} and 2^s there are at least two primes. On the other hand, if n is a natural number with the property $2^{s-1} \leqslant n < 2^s$, then it has, of course, s digits in the scale of 2.

4. Prove that the last digit of the representation as a decimal in the scale of 12 of any arbitrary square is a square.

PROOF. If the last digit of a natural number is 0, 1, ..., 11, then the last digit (in the scale of 12) of the square of it is 0, 1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1, respectively. □

REMARK. It has been proved that other scales with this property (proved above for the scale of 12) are only the numbers 2, 3, 4, 5, 8, 16. Cf. Müller [1].

5. Prove that there exist infinitely many natural numbers n that are not divisible by 10 and such that number n', obtained from n by reversing the order of the digits in the representation of n as a decimal in the scale of 10, is a divisor of n and $n:n' > 1$.

PROOF. As is easy to verify, the following numbers have the desired property:

$$9899\ldots9901 = 9\cdot 1099\ldots9989$$

and

$$8799\ldots9912 = 4\cdot 2199\ldots9978$$

where the number of 9's in the middle is arbitrary but equal on either side of the equality.

It can be proved that the least natural number > 9 with this property is the number $8712 = 4\cdot 2178$ and that the numbers written above exhaust the class of the numbers of this property. Cf. Subba Rao [1]. The problem whether such numbers exist had been formulated by D. R. Kaprekar. □

6. Prove that any natural number may be uniquely expressed in the form

$$(*)\qquad n = a_1\cdot 1!+a_2\cdot 2!+ \ldots +a_m\cdot m!,$$

where m is a natural number, $a_m \neq 0$ and a_j $(j = 1, 2, \ldots, m)$ are integers such that $0 \leqslant a_j \leqslant j$ for $j = 1, 2, \ldots, m$.

PROOF. Suppose that a natural number n admits two representations in the form $(*)$. We then have

$$a_1\cdot 1!+a_2\cdot 2!+ \ldots +a_m\cdot m! = a_1'\cdot 1!+a_2'\cdot 2!+ \ldots +a_m'\cdot m!.$$

Let k denote the greatest natural number such that $a_k \neq a_k'$, i.e. $a_k' > a_k$, say. Therefore $a_k'-a_k \geqslant 1$, whence

$$k! \leqslant a'_k \cdot k! - a_k \cdot k! = a_1 \cdot 1! + \dots + a_{k-1}(k-1)! - a'_1 \cdot 1! - \dots - a'_{k-1}(k-1)!$$
$$\leqslant 1 \cdot 1! + 2 \cdot 2! + \dots + (k-1)(k-1)! = k! - 1 < k!,$$

which is impossible.

Now let s denote a natural number. Consider all the expansions of the form $(*)$ with $m \leqslant s$ and $0 \leqslant a_j \leqslant j$ for $j = 1, 2, \dots, m$. As is easy to calculate, the number of them is equal to $(1+1)(2+1)\dots(s+1) = (s+1)!$. Therefore the number of the expansions excluding those which give $n = 0$ is $(s+1)! - 1$. In virtue of what we have proved above, different expansions of the form $(*)$ give different n's. On the other hand, any expansion of the form $(*)$ with $m \leqslant s$ produces a natural number $\leqslant 1 \cdot 1! + 2 \cdot 2! + \dots + m \cdot m! = (m+1)! - 1 \leqslant (s+1)! - 1$. Hence, trivially, any natural number $\leqslant (s+1)! - 1$ can be obtained as an n for a suitable expansion of the form $(*)$ with $m \leqslant s$. ☐

7. For fixed natural numbers g and s let $f(n)$ denote the sum of the sth powers of the digits in the scale of g of the natural number n. Prove that for any natural number n the infinite sequence

$$\text{(i)} \qquad n, f(n), ff(n), fff(n), \dots$$

is periodic.

PROOF. Clearly, in order to show that sequence (i) is periodic it is sufficient to prove that there is a number which occurs as distinct terms of (i).

In other words, it is sufficient to prove that not all terms of (i) are different. Let n denote a natural number and let $n = a_0 + a_1 g + \dots + a_{k-1} g^{k-1}$ be the representation of n as a decimal in the scale of g. We have $f(n) = a_0^s + a_1^s + \dots + a_{k-1}^s \leqslant k(g-1)^s < kg^s$. But, as we know, g^k/k increases to infinity with k; so for k large enough we have $g^k/k > g^{s+1}$. Therefore $kg^s < g^{k-1} \leqslant n$. From this we easily infer that for sufficiently large n, say for $n > m$, we have $f(n) < n$. This shows that after any term of the sequence that is greater than m there occurs a term less than the term in question. Consequently, for none of the terms all the terms that follow it are greater than m (for this would produce a decreasing infinite sequence of natural numbers). Thus we have proved that the sequence contains infinitely many terms that are not greater than m and this shows that the sequence must contain distinct terms that are equal, and this is what was to be proved. ☐

REMARK. For $g = 10$ and $s = 2$, Porges [1] has proved that the period of sequence (i) consists of either one term equal to 1 or the following eight terms: 4, 16, 37, 58, 89, 145, 42, 20. For example, if $n = 3$ we have the sequence 3, 9, 81, 65, 61, 37, 58, ..., 16, 37, ...; if $n = 5$, we have the sequence 5, 25, 29, 85, 89, 145, ..., 58, 89, ...; if $n = 7$, we have the sequence 7, 49, 97, 130, 10, 1, 1, 1, ... A generalization of the results of Porges has been obtained by B. M. Stewart [1]. The case where $g = 10$ and $s = 3$ has been considered by K. Iséki [1]. He has proved that there are 9 possible periods of the sequence of the form (i). These are: one term periods, the term being any of the numbers 1, 153, 370, 371, 407; period consisting of two numbers, either of 136 and 244 or of 919 and 1459; finally, periods consisting of three numbers, either of 55, 250, 133 or of 160, 217, 252 (see also Iséki [2]).

K. Chikawa, K. Iséki and T. Kusakabe [1] proved that in the case where $g = 10, s = 4$ there are six possible periods of sequence (i). These are: periods consisting of one number, which can be any of the numbers 1, 1634, 8208, 9474; a period consisting of the numbers 2178, 6514; a period consisting of seven numbers 13139, 6725, 4338, 4514, 1138, 4179, 9219 (Chikawa, Iséki, Kusakabe and Shibamura [1] found all periods for $g = 10$, $s = 5$, Avanesov, Gusev [1] for $g = 10$, $s = 6$ or 7, Takada [1] for $g = 10$, $s = 8$, Iséki and Takada [1] for $g = 10, s = 9$ and finally Avanesov, Gusev [2] for $g = 10, s = 10$ or 11).

8. Prove that the period of sequence (i) of exercise 7 may begin arbitrarily far.

PROOF. This follows immediately from the fact that for every natural number n there exists a natural number $m > n$ such that $f(m) = n$. In fact, for any natural number s the sum of the s-th powers of the digits (in the scale of g) of the number $m = \frac{g^n - 1}{g-1}$ is n and, moreover, if $n > 1$, we have $m > n$; if $n = 1$, then we put $m = g$. ☐

9. Find the tables of addition and multiplication of decimals in the scale of 7.

ANSWER:

	1	2	3	4	5	6
1	2	3	4	5	6	10
2	3	4	5	6	10	11
3	4	5	6	10	11	12
4	5	6	10	11	12	13
5	6	10	11	12	13	14
6	10	11	12	13	14	15

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

2. Representations of numbers by decimals in negative scales

THEOREM 2. *If g is an integer < -1, then any integer $N \neq 0$ may be uniquely expressed as a decimal of form* (1), *where c_n $(n = 0, 1, \ldots, m)$ are integers such that*

$$(7) \qquad 0 \leqslant c_n < |g| \quad \textit{for} \quad n = 0, 1, \ldots, m$$

and $c_m \neq 0$.

The theorem is due to Z. Pawlak and Andrzej Wakulicz [1], who have found it as an aid to computation with the use of electronic computers.

PROOF. Let g be an integer < -1 and $x = N$ an arbitrary integer. Denote by c_0 the remainder left when x is divided by $|g|$. We have $0 \leqslant c_0 < |g|$ and $x = c_0 + gx_1$, where x_1 is an integer. Hence $gx_1 = x - c_0$ and so $|gx_1| \leqslant |x| + c_0 \leqslant |x| + |g| - 1$, whence $|x_1| \leqslant (|x| + |g| - 1)/|g|$. If $(|x| + |g| - 1)/|g| \geqslant |x|$, then $|x| + |g| - 1 \geqslant |g|\,|x|$, i.e. $|g| - 1 \geqslant (|g| - 1)\,|x|$, whence, by $|g| > 1$, we see that $|x| \leqslant 1$, so $x = 0, 1$ or -1. If $x = 0$ or $x = 1$, then $x = c_0$. If $x = -1$, then $x \doteq |g| - 1 + g = c_0 + g$, where $c_0 = |g| - 1$. Therefore it remains to consider the case where $(|x| + |g| - 1)/|g| < |x|$. We have $|x_1| < |x|$ and we may apply the procedure which we have just applied to x, to x_1. Continuing, we proceed in this way until, after a finite number of steps, we obtain a representation of N in form (1), where c_n ($n = 0, 1, \ldots, m$) are integers satisfying conditions (7).

In order to prove that the representation of N in form (1), conditions (7) being satisfied, is unique, it is sufficient to note that N divided by $|g|$ leaves the remainder c_0, $(N - c_0)/g$ divided by $|g|$ leaves the remainder c_1 and so on. Hence it follows that the numbers c_0, c_1, c_2, ... are uniquely defined by number N; so the representation of N in form (1) is unique. Theorem 2 is thus proved.

EXAMPLES: $-1 = (11)_{-2}$, $10 = (11110)_{-2}$, $-10 = (1010)_{-2}$, $16 = (10000)_{-2}$, $-16 = (110000)_{-2}$, $25 = (1101001)_{-2}$, $-25 = (111011)_{-2}$, $100 = (110100100)_{-2} = (10201)_{-3}$.

3. Infinite fractions in a given scale

Let g denote a natural number >1 and x a real number. Let $x_1 = x - [x]$. We have $0 \leqslant x_1 < 1$. Further, let $x_2 = gx_1 - [gx_1]$, then again $0 \leqslant x_2 < 1$. Continuing, we define x_3 as $gx_2 - [gx_2]$ and so on. Thus we obtain an infinite sequence x_n ($n = 1, 2, \ldots$) defined by the conditions

$$(8)\qquad x_1 = x - [x], \qquad x_{n+1} = gx_n - [gx_n] \quad \text{for} \quad n = 1, 2, \ldots$$

These formulae imply

$$(9)\qquad 0 \leqslant x_n < 1 \quad \text{for} \quad n = 1, 2, \ldots$$

Let

$$(10)\qquad c_n = [gx_n] \quad \text{for} \quad n = 1, 2, \ldots$$

In virtue of (9) we have $0 \leqslant gx_n < g$; therefore, by (10), $0 \leqslant c_n < g$, and, since numbers (10) are integers, we have

$$(11)\qquad 0 \leqslant c_n \leqslant g - 1 \quad \text{for} \quad n = 1, 2, \ldots$$

Formulae (8) and (11) give

$$x = [x] + x_1, \qquad x_1 = \frac{c_1 + x_2}{g}, \qquad x_2 = \frac{c_2 + x_3}{g}, \qquad \ldots,$$
$$x_n = \frac{c_n + x_{n+1}}{g}.$$

Hence, for $n = 1, 2, \ldots$,

$$(12)\qquad x = [x] + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n} + \frac{x_{n+1}}{g^n}.$$

Since, by (9), $0 \leqslant \dfrac{x_{n+1}}{g^n} < \dfrac{1}{g^n}$ and in virtue of $g \geqslant 2, g^n$ increases to infinity with n, we see that $\lim\limits_{n\to\infty} \dfrac{x_{n+1}}{g^n} = 0$. Therefore, by (12), we obtain the following expansion of number x into an infinite series:

$$x = [x] + \frac{c_1}{g} + \frac{c_2}{g^2} + \frac{c_3}{g^3} + \ldots \tag{13}$$

where, by (11), numbers c_n are digits in the scale of g.

Thus we have proved that every real number x has a representation (at least one) in form (13) for any given natural scale $g > 1$, where numbers c_n are digits in the scale of g.

Suppose that a real number x is represented in form (13) (where c_n are integers satisfying conditions (11)). For any $n = 1, 2, \ldots$ we set

$$r_n = [x] + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_n}{g^n}. \tag{14}$$

We have

$$x - r_n = \frac{c_{n+1}}{g^{n+1}} + \frac{c_{n+2}}{g^{n+2}} + \ldots,$$

whence, by (11),

$$0 \leqslant x - r_n \leqslant \frac{g-1}{g^{n+1}} + \frac{g-1}{g^{n+2}} + \ldots = \frac{1}{g^n},$$

the equality $x - r_n = 1/g^n$ being possible only in the case where $c_{n+1} = c_n = \ldots = g-1$, i.e. where all the digits of the representation are equal to $g - 1$ from a certain n onwards. Then $x = r_n + 1/g^n$, and so, by (14), x is the quotient of an integer by a power of number g. If m is the least natural number such that $c_n = g-1$ for $n \geqslant m$, then in the case of $m = 1$, by (13), we would have $x = [x] + 1$, which is impossible. If, however, $m > 1$, then $c_{m-1} \neq g-1$, therefore, by (11), $c_{m-1} < g-1$, that is, $c_{m-1} \leqslant g-2$, which shows that number $c'_{m-1} = c_{m-1} + 1$ is also a digit in the scale of g; consequently number x has a representation

$$x = [x] + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_{m-2}}{g^{m-2}} + \frac{c'_{m-1}}{g^{m-1}} + \frac{0}{g^m} + \frac{0}{g^{m+1}} + \ldots,$$

which is different from (13).

It is easy to prove that, conversely, if x is the quotient of an integer by a power of number g, then x has two different representations in form (13), where c_n are integers satisfying conditions (11). In one of them all c_n's except a finite number are equal to zero, in the other from a certain n onwards all c_n's are equal to $g-1$.

If a real number x is not the quotient of an integer by a power of number g, then

$$0 \leqslant x - r_n < \frac{1}{g^n} \quad \text{for} \quad n = 1, 2, \ldots,$$

whence $0 \leqslant g^n x - g^n r_n < 1$. Hence, since by (14) number $g^n r_n$ is an integer, we see that $g^n r_n = [g^n x]$, this being also true for $n = 0$ provided r_0 is defined as $[x]$. We then have

$$g^n r_n = [g^n x] \quad \text{and} \quad g^{n-1} r_{n-1} = [g^{n-1} x] \qquad (15)$$
$$\text{for} \quad n = 1, 2, \ldots$$

But, in view of (14), $r_n - r_{n-1} = \frac{c_n}{g^n}$ for any $n = 1, 2, \ldots$, whence $c_n = g^n r_n - g g^{n-1} r_{n-1}$ which, by (15), implies

$$c_n = [g^n x] - g[g^{n-1} x], \quad n = 1, 2, \ldots \qquad (16)$$

This shows that any real number x which is not the quotient of an integer by a power of g has precisely one representation as series (13), where c_n are integers satisfying conditions (11). This representation is denoted by

$$x = [x] + (0, c_1 c_2 c_3 \ldots)_g \,. \qquad (17)$$

Formula (16), which gives the nth digit, is simple; however, it is not easy in general to compute the value of its right-hand side. For example, for $g = 10$ formula (16) gives for the 1000th digit of the decimal of $\sqrt{2}$ the value $c_{1000} = [10^{1000}\sqrt{2}] - 10[10^{999}\sqrt{2}]$, which is not easy to calculate.

We have just proved that in order to obtain the representation of a real number as a decimal (17) we may apply the following algorithm: $x_1 = x - [x]$, $c_1 = [gx_1]$, $x_2 = gx_1 - c_1$, $c_2 = [gx_2]$, $x_3 = gx_2 - c_2, \ldots,$ $x_n = gx_{n-1} - c_{n-1}$, $c_n = [gx_n], \ldots$

We have also proved that representation (13) is finite (i.e. all its digits are zero from a certain n onwards) if and only if x is the quotient of an integer by a power of number g. It is easy to prove that this condition is equivalent to saying that x is a rational number equal to an irreducible fraction whose denominator is a product of primes each of which is a divisor of g. The necessity of this condition is evident. On the other hand, if $x = l/m$, where l is an integer and m a natural number such that any prime divisor of m is a divisor of g, then, if $g = q_1^{\alpha_1}q_2^{\alpha_2}\dots q_s^{\alpha_s}$ denotes the factorization of g into primes, $m = q_1^{\lambda_1}q_2^{\lambda_2}\dots q_s^{\lambda_s}$, where $\lambda_1, \lambda_2, \dots, \lambda_s$ are non-negative integers. Let k be a natural number such that $k\alpha_i \geqslant \lambda_i$ for any $i = 1, 2, \dots, s$. Then $m \mid g^k$, so $g^k = hm$ where h is a natural number. Hence $x = l/m = hl/g^k$, which gives the sufficiency of the condition.

Thus we see that if a real number x is not a rational number which is an irreducible fraction with a denominator such that any prime divisor of it divides g, then number x has precisely one representation in form (13), where c_n $(n = 1, 2, \dots)$ are digits in the scale of g. Moreover, the representation is infinite and has infinitely many digits different from $g-1$. The representation is to be obtained by the use of the algorithm presented above.

The algorithm for representing a real number x as a decimal may also be applied in the case where g is a real number > 1. Then formuale (8), (9), (10) and (12) are still valid. However, the only proposition about c_n's $(n = 1, 2, \dots)$ which remains true is that they satisfy the inequalities $0 \leqslant c_n < g$ and that they are integers. For example, for $g = \sqrt{2}$, $x = \sqrt{2}$ the representation given by the algorithm is

$$\sqrt{2} = 1 + \frac{1}{(\sqrt{2})^3} + \frac{1}{(\sqrt{2})^9} + \frac{1}{(\sqrt{2})^{12}} + \frac{1}{(\sqrt{2})^{21}} + \dots$$

However, there is also another representation of $\sqrt{2}$ in the form (13). This is

$$\sqrt{2} = \frac{1}{\sqrt{2}} + \frac{1}{(\sqrt{2})^3} + \frac{1}{(\sqrt{2})^5} + \frac{1}{(\sqrt{2})^7} + \dots$$

For $g = \sqrt{2}$ and $x = (2\sqrt{2}+1)/4$ we have two representations in the form (13):

$$\frac{2\sqrt{2}+1}{4} = \frac{1}{\sqrt{2}} + \frac{1}{(\sqrt{2})^6} + \frac{1}{(\sqrt{2})^8} + \dots = \frac{1}{\sqrt{2}} + \frac{1}{(\sqrt{2})^4} + \dots,$$

the latter being given by the algorithm. We also have

$$\begin{aligned}\frac{1}{2} + \frac{\sqrt{2}}{4} &= \frac{1}{(\sqrt{2})^4} + \frac{1}{(\sqrt{2})^5} + \frac{1}{(\sqrt{2})^6} + \dots \\ &= \frac{1}{(\sqrt{2})^2} + \frac{1}{(\sqrt{2})^5} + \frac{1}{(\sqrt{2})^7} + \dots\end{aligned}$$

where the second representation is given by the algorithm. See also Gelfond [1].

4. Representations of rational numbers by decimals

Now let x be a rational number which is equal to an irreducible fraction l/m and suppose that the representation of x as a decimal is of the form (13), where c_n $(n = 1, 2, \dots)$ are digits in the scale of g where g is an integer > 1. Let x_n $(n = 1, 2, \dots)$ be numbers defined by formulae (8). Then, as we know, formulae (9) and (10) hold. In virtue of (8) we have $mx_1 = l - [x]$. Consequently mx_1 is a natural number and, since, by (8), we have $mx_{n+1} = gmx_n - m[gx_n]$ for any $n = 1, 2, \dots$, then by induction, we infer that all the numbers mx_n are integers and, moreover, by (9), that they satisfy the inequalities $0 \leqslant mx_n < m$ for $n = 1, 2, \dots$ If for some n we have $x_n = 0$, then, by (8), $x_j = 0$ for all $j \geqslant n$. Hence, by (10), $c_j = 0$ for $j \geqslant n$ and representation (13) for x is finite. Further, suppose that $x_n \neq 0$ for all $n = 1, 2, \dots$ We then have $0 < mx_n < m$ for $n = 1, 2, \dots$ and so the numbers $mx_1, mx_2, \dots, mx_m$ can take only $m-1$ different values $1, 2, \dots, m-1$. It follows that there exist natural numbers h and s such that $h+s \leqslant m$ and $mx_h = mx_{h+s}$, which, by (8), proves that $x_n = x_{n+s}$ for $n > h$ and therefore, by (10), $c_n = c_{n+s}$ for $n \geqslant h$. This proves that the infinite sequence of digits in (17) is periodic. We have thus proved the following theorem:

THEOREM 3. *The representation of a rational number in form* (13), *where g is a natural number greater than* 1, *is periodic. The number of digits in the period, as well as the number, not less than* 0, *of digits preceding the period, is less than the denominator of the rational number in question.*

Consider an arbitrary infinite sequence $c_1, c_2, \dots$, where $c_n (n = 1, 2, \dots)$ are digits in the scale of g. Then the c_n's satisfy condition (11), whence it follows that infinite series (13) is convergent and its sum x is a real number. It follows from Theorem 3 that, if the sequence $c_1, c_2, \dots$ is not periodic, then x is an irrational number. In order to prove the converse it is sufficient to show that if a sequence of digits $c_1, c_2, \dots$ is periodic, then number (17) is rational.

Suppose then that the sequence $c_1, c_2, \dots$ is periodic. This means that for some natural numbers s and h the equality $c_{n+s} = c_n$ holds whenever $n \geqslant h$. We then have

$$\frac{c_1}{g} + \frac{c_2}{g^2} + \ldots$$

$$= \frac{c_1}{g} + \frac{c_2}{g^2} + \frac{c_{h-1}}{g^{h-1}} + \frac{c_h}{g^h} + \frac{c_{h+1}}{g^{h+1}} + \ldots +$$

$$+ \frac{c_{h+s-1}}{g^{h+s-1}} + \frac{c_h}{g^{h+s}} + \frac{c_{h+1}}{g^{h+s+1}} + \ldots + \frac{c_{h+s-1}}{g^{h+2s-1}} + \ldots$$

$$= \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_{h-1}}{g^{h-1}} + \left(\frac{c_h}{g^h} + \frac{c_{h+1}}{g^{h+1}} + \ldots + \frac{c_{h+s-1}}{g^{h+s-1}}\right) \times$$

$$\times \left(1 + \frac{1}{g^s} + \frac{1}{g^{2s}} + \ldots\right)$$

$$= \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots + \frac{c_{h-1}}{g^{h-1}} + \left(\frac{c_h}{g^h} + \frac{c_{h+1}}{g^{h+1}} + \ldots + \frac{c_{h+s-1}}{g^{h+s-1}}\right) \frac{g^s}{g^s - 1}$$

$$= \frac{c_1 g^{h+s-2} + c_2 g^{h+s-3} + \ldots + c_{h-1} g^s + c_h g^{s-1} + \ldots + c_{h+s-1}}{g^{h-1}(g^s - 1)} -$$

$$- \frac{c_1 g^{h-1} + c_2 g^{h-2} + \ldots + c_{h-1}}{g^{h-1}(g^s - 1)}$$

$$= \frac{(c_1 c_2 \ldots c_{h+s-1})_g}{g^{h-1}(g^s - 1)} - \frac{(c_1 c_2 \ldots c_{h-1})_g}{g^{h-1}(g^s - 1)}.$$

Thus we see that the sum of the series is a rational number

$$\frac{(c_1 c_2 \ldots c_{h+s-1})_g - (c_1 c_2 \ldots c_{h-1})_g}{g^{h-1}(g^s - 1)}.$$

This, however, in the form as is written, is not necessarily an irreducible fraction.

This formula may also serve as a *rule for reducing periodic fractions* in a given scale of $g > 1$.

We have thus proved the following

THEOREM 3^a. *For a given scale of $g > 1$, where g is a natural number, the numbers which admit representations in form* (13) *such that the sequence of the digits is periodic are precisely rational numbers* (finite representations are understood to be periodic, the period consisting of one number being equal either to 0 or to $g - 1$).

As an immediate consequence of Theorem 3^a we note that if a number x has a non-periodic representation as a decimal in a scale of g, then x is irrational. On the basis of this fact it is easy to prove that a number a whose decimal (in the scale of 10) is obtained by writing 0 for the integer and the consecutive natural numbers to the right of the decimal point, i.e. number

$$a = 0.1234567891011121314\ldots,$$

is an irrational number. In fact, if the decimal of a were recurring, then, since all numbers 10^n $(n = 1, 2, \ldots)$ occur in it, arbitrarily long sequences consisting of 0's would appear; consequently, the period would necessarily consist of number 0 only. But this is impossible since infinitely many 1's occur in the decimal.

EXERCISES. 1. Write the number $\frac{1}{99^2}$ as a decimal.

ANSWER:

$$\frac{1}{99^2} = 0.\dot{0}\dot{0}\dot{0}\dot{1}\dot{0}\dot{2}\dot{0}\dot{3}\ldots\dot{0}\dot{8}\dot{0}\dot{9}\dot{1}\dot{0}\dot{1}\dot{1}\dot{1}\dot{2}\ldots\dot{9}\dot{6}\dot{9}\dot{7}\dot{9}\dot{9}.$$

(the dots above the digits indicate that the digits form the period). The period (which starts exactly at the decimal point) is obtained by writing down all the natural numbers from 0 to 99 excluding 98 written as decimals. As proved by J. W. L. Glaisher [1] a more general formula holds

$$\frac{1}{(g-1)^2} = (0.\dot{0}\dot{1}\dot{2}\dot{3}\ldots\overline{\dot{g-3}}\;\overline{\dot{g-1}})_g$$

whenever g is a natural number > 2.

2. Using the representation of the number e as a decimal $e = 2.718281828\ldots$ write the number e as a decimal in the scale of 2 up to the 24th decimal place.

ANSWER:

$$e = (10.101101111110000101010001\ldots)_2.$$

This representation has been given by G. Peano [1], p. 154. He writes a point and an exclamation mark in place of 0 and 1, respectively; therefore this equality has the form

$$e = (!.,!.!!.!!!!!!....!.!.!...!)_2.$$

3. Using the representation of the number π as a decimal $\pi = 3.14159265\ldots$ write the number π as a decimal in the scale of 2 up to the 24th decimal place.

ANSWER:

$$\pi = (11.001001000011111101101010\ldots)_2$$

(cf. G. Peano [1], p. 177).

4. Prove that in any infinite decimal fraction there are arbitrarily long sequences of digits that appear infinitely many times.

PROOF. Let $0.c_1c_2c_3\ldots$ denote an infinite decimal fraction and m a natural number. Consider all the blocks of m digits which appear in the sequence $c_1c_2\ldots$, i.e. all the sequences

$$c_{km+1}, c_{km+2}, \ldots, c_{km+m} \quad \text{where} \quad k = 0, 1, \ldots \tag{18}$$

We divide the set of sequences into classes by saying that two sequences belong to the same class if and only if the terms of one are equal to the corresponding terms of the other. Clearly, the number of classes of sequences consisting of m terms is not greater than 10^m. Consequently it is a finite number. But, on the other hand, there are infinitely many sequences of form (18); so at least one of the classes contains infinitely many of them. ☐

REMARK. As a special case of the theorem just proved, we note that in any infinite decimal fraction at least one digit appears infinitely many times. (If, moreover, the number is irrational, there are at least two digits that appear infinitely many times each). However, for the numbers $\sqrt{2}$ and π we are unable to establish which two of the digits have this property. As was noticed by L. E. J. Brouwer, we do not know whether the sequence 0123456789 appears in the representation of number π as a decimal.

The decimals of e and π up to the 100000th decimal place are to be found in Shanks and Wrench [2] and [1], respectively.

The number π is given up to the 1000000th decimal place in Gilloud and Bourger [1] and to 4196239 in Tamura and Kanada [1].

5. Prove that the number $(cc\ldots c)_{10}$, whose digits in the scale of 10 are all equal to c, with $c = 2$, $c = 5$ or $c = 6$, is not of the form m^n, where m and n are natural numbers > 1.

PROOF. Numbers 2, 5 and 6 are not divisible by any square of a natural number > 1. Therefore none of them can be of the form m^n, where m and n are natural numbers > 1. Numbers whose last two digits are 22, 55 or 66 are not divisible by the numbers 4, 25 and 4 respectively, which would be the case if they were of the form m^n, where m and n are natural numbers > 1. A number > 4 whose digits (in the scale of 10) are all equal to 4 is divisible by 4 but not divisible by 8. Consequently it cannot be an nth power of a natural number m with $n \geqslant 3$. If $44\ldots4 = m^2$, then the number $11\ldots1$ would be a square; but this is impossible since the last two digits of a square of a natural number cannot be 11. ☐

REMARK. R. Obláth [1] showed that, if any of the numbers 33...3, 77...7, 88...8, 99...9 is greater than 10, then it cannot be of the form m^n, where m, n are natural numbers > 1. It is still an open question whether the number 11...1 can be of that form, see Shorey and Tijdeman [1]).

6. Write the number $\frac{1}{10}$ as a decimal in the scale of 2 and in the scale of 3.

ANSWER:

$$\tfrac{1}{10} = (0.0\dot{0}\dot{0}\dot{1}\dot{1})_2 = (0.\dot{0}\dot{0}\dot{2}\dot{2})_3.$$

7. Write the number $\frac{1}{61}$ as a decimal in the scale of 10.

ANSWER:

$$\tfrac{1}{61} = (0.\dot{0}\dot{1}\dot{6}\dot{3}\dot{9}\dot{3}\dot{4}\dot{4}\dot{2}\dot{6}\dot{2}\dot{2}\dot{9}\dot{5}\dot{0}\dot{8}\dot{1}\dot{9}\dot{6}\dot{7}\dot{2}\dot{1}\dot{3}\dot{1}\dot{1}\dot{4}\dot{7}\dot{5}\dot{4}\dot{0}\dot{9}\dot{8}\dot{3}\dot{6}\dot{0}\dot{6}\dot{5}\dot{5}\dot{7}\dot{3}\dot{7}\dot{7}\dot{0}\dot{4}\dot{9}\dot{1}\dot{8}\dot{0}\dot{3}\dot{2}\dot{7}\dot{8}\dot{6}\dot{8}\dot{8}\dot{5}\dot{2}\dot{4}\dot{5}\dot{9})_{10}.$$

REMARK. It can be proved that the period of the decimal of the number 1/97 consists of 96 digits and that of the number 1/1913 consists of 1912 digits. We do not know whether there exist infinitely many natural numbers $n > 2$ such that the decimal of the number $1/n$ has the period consisting of $n-1$ digits. To this class belong the numbers $n = 313, 1021, 1873, 2137, 3221, 3313$. It can be proved that primes for which 10 is a primitive root have this property.

5. Normal numbers and absolutely normal numbers

Let g be a natural number > 1; we write a real number $x: x = [x] + (0.c_1\, c_2\, c_3 \ldots)_g$ as a decimal in the scale of g. For any digit c (in the scale of g) and every natural number n we denote by $l(c, n)$ the number of those digits of the sequence $c_1, c_2, \ldots, c_n$ which are equal to c. If

$$\lim_n \frac{l(c, n)}{n} = \frac{1}{g}$$

for each of the g possible values of c, then the number x is called *normal* in the scale of g. For example number

$$\frac{1234567890}{9999999999}$$

is normal in the scale of 10; number $\frac{1}{10}$ is normal in the scale of 2 but it is not normal in the scale of 3. If x is a normal number in the scale of 10, then $x/2$ is not necessarily a normal number. For example, $x = 0.\dot{1}\dot{3}\dot{5}\dot{7}\dot{9}\dot{8}\dot{2}\dot{0}\dot{4}\dot{6}$ is normal and $x/2 = 0.\dot{0}\dot{6}\dot{7}\dot{8}\dot{9}\dot{9}\dot{1}\dot{0}\dot{2}\dot{3}$ is not.

A number which is normal in any scale is called *absolutely normal*. The existence of absolutely normal numbers was proved by E. Borel [1]. His proof is based on the measure theory and, being purely existentional, it does not provide any method for constructing such a number. The first effective example of an absolutely normal number was given by me in the year 1916 (Sierpiński [5], see also H. Lebesgue [1]). As was proved by Borel, almost all (in the sense of the measure theory) real numbers are absolutely normal. However, as regards most of the commonly used numbers, we either know them not to be normal or we are unable to decide whether they are normal or not. For example, we do not know whether the numbers $\sqrt{2}$, π, e are normal in the scale of 10. Therefore, though according to the theorem of Borel almost all numbers are absolutely normal, it was by no means easy to construct an example of an absolutely normal number. Examples of such numbers are indeed fairly complicated.

D. G. Champernowne [1] proved in 1933 that the number a (which we proved in § 4 to be irrational) is normal in the scale of 10. He formulated the conjecture that the number whose decimal is obtained by writing 0 for the integers and the consecutive prime numbers (instead of consecutive natural numbers) to the right of the decimal point, i.e. number 0.2357111317..., is normal in the scale of 10. The conjecture, and a more general theorem have been proved by A. H. Copeland and P. Erdös [1]. Other interesting properties of normality have been investigated by W. M. Schmidt [1].

6. Decimals in the varying scale

Let $g_1, g_2, \ldots$ be an infinite sequence of natural numbers > 1, x a real number. We define infinite sequences $c_1, c_2, \ldots$ and $x_1, x_2, \ldots$ as follows:

$$\begin{aligned} &c_0 = [x],\; x_1 = x - c_0, \quad c_1 = [g_1 x_1],\; x_2 = g_1 x_1 - c_1, \\ &c_2 = [g_2 x_2], \ldots,\; c_n = [g_n x_n],\; x_{n+1} = g_n x_n - c_n, \quad n = 1, 2, \ldots \end{aligned} \tag{19}$$

It is clear that $0 \leqslant x_n < 1$ and $0 \leqslant c_n \leqslant g_n - 1$ hold for any $n = 1, 2, \ldots$

Comparing formulae (19) and the algorithm of § 3, we see that the digit c_1 has been defined as if it were the corresponding digit in the scale of g_1, c_2 as if it were the corresponding digit in the scale of g_2 and so on. Moreover, formulae (19) give

(20)
$$x = c_0 + \frac{c_1}{g_1} + \frac{c_2}{g_1 g_2} + \frac{c_3}{g_1 g_2 g_3} + \ldots + \frac{c_n}{g_1 g_2 \cdots g_n} + \frac{x_{n+1}}{g_1 g_2 \cdots g_n}.$$

Since for $n = 1, 2, \ldots$ we have $g_n \geqslant 2$ and $0 \leqslant x_{n-1} < 1$, the last summand in (20) is non-negative and less than $1/2^n$, and consequently it tends to zero as n increases to infinity. This gives the following expansion of number x in an infinite series:

$$x = c_0 + \frac{c_1}{g_1} + \frac{c_2}{g_1 g_2} + \frac{c_3}{g_1 g_2 g_3} + \ldots \tag{21}$$

If $g_1 = g_2 = \ldots = g$, this coincides with the ordinary representation of x as a decimal in the scale of g.

Now we put $g_n = n+1$, $n = 1, 2, \ldots$ Then (21) assumes the form

$$x = c_0 + \frac{c_1}{2!} + \frac{c_2}{3!} + \frac{c_3}{4!} + \ldots, \tag{22}$$

where c_0, c_n $(n = 1, 2, ...)$ are integers and

$$0 \leqslant c_n < n \quad (n = 1, 2, ...). \tag{23}$$

It is easy to prove that if x is a rational, algorithm (19) leads to a finite representation in form (22), where c_n $(n = 1, 2, ...)$ satisfy inequalities (23). However, any rational admits also another infinite representation in form (22). This follows from the following identity:

$$c_0 + \frac{c_1}{2!} + \frac{c_2}{3!} + ... + \frac{c_{n-1}}{n!} + \frac{c_n}{(n+1)!}$$

$$= c_0 + \frac{c_1}{2!} + ... + \frac{c_{n-1}}{n!} + \frac{c_n - 1}{(n+1)!} + \frac{n+1}{(n+2)!} + \frac{n+2}{(n+3)!} + \frac{n+3}{(n+4)!} + ...$$

As regards representations of type (21) see E. Strauss [1] and G. Cantor [1]; representations of the type (22) have been investigated by C. Stéphanos [1] and G. Faber [1].

Let us mention some other expansions of real numbers into infinite series.

Let x denote a positive real number. Denote by k_1 the least natural number satisfying the inequality $k_1 x > 1$. We set $k_1 x = 1 + x_1$ and have $x_1 > 0$. We proceed similarly with x_1 in place of x, i.e. we find the least natural number k_2 such that $k_2 x_1 > 1$ and we put $k_2 x_1 = 1 + x_2$ and so on. The expansion of x into an infinite series thus obtained is as follows

$$x = \frac{1}{k_1} + \frac{1}{k_1 k_2} + \frac{1}{k_1 k_2 k_3} + ...,$$

where $k_n (n = 1, 2, ...)$ are natural numbers and $k_{n+1} \geqslant k_n$ for $n = 1, 2, ...$

It can be proved that each positive real number has precisely one representation in this form and that a sufficient and necessary condition for x to be an irrational number is that $\lim_{n\to\infty} k_n = +\infty$ (Sierpiński [3]).

The expansion thus obtained for the number e is as follows:

$$e = \frac{1}{1} + \frac{1}{1\cdot 1} + \frac{1}{1\cdot 1\cdot 2} + \frac{1}{1\cdot 1\cdot 2\cdot 3} + ...$$

Let a be a natural number > 2. Using the identity

$$\frac{a - \sqrt{a^2-4}}{2} = \frac{1}{a} + \frac{a^2 - 2 - \sqrt{(a^2-2)^2 - 4}}{2a}$$

one easily proves that for $a_1 = a$, $a_{n+1} = a_n^2 - 2\,(n = 1, 2, \ldots)$

$$\frac{a-\sqrt{a^2-4}}{2} = \frac{1}{a_1} + \frac{1}{a_1 a_2} + \frac{1}{a_1 a_2 a_3} + \ldots \tag{24}$$

This series converges rapidly because, as is easily proved by induction, $a_n > 2^{2^{n-1}}$, $n = 1, 2, \ldots$

In particular, for $a = 3$, we obtain $a_1 = 3, a_2 = 7, a_3 = 47, a_4 = 2207$, $a_5 = 4870847$ and so on. Hence

$$\frac{3-\sqrt{5}}{2} = \frac{1}{3} + \frac{1}{3\cdot 7} + \frac{1}{3\cdot 7\cdot 47} + \frac{1}{3\cdot 7\cdot 47\cdot 2207} + \ldots$$

This expansion is to be found under the name of *Pell's series* in a book by E. Lucas [2], p. 331.

If a is even, $a = 2b, b > 1$, from (24) we derive the following expansion:

$$b-\sqrt{b^2-1} = \frac{1}{2b_1} + \frac{1}{2b_1\,2b_2} + \frac{1}{2b_1\,2b_2\,2b_3} + \ldots$$

where $b_1 = b$ and $b_{n+1} = 2b_n^2 - 1$ for $n = 1, 2, \ldots$

It is worth noticing that the following expansion into an infinite product is valid:

$$\sqrt{\frac{b+1}{b-1}} = \left(1+\frac{1}{b_1}\right)\left(1+\frac{1}{b_2}\right)\left(1+\frac{1}{b_3}\right)\ldots$$

Some particular cases of this expansion (for $b = 2$, $b = 3$ and some others) were given by G. Cantor [2] in 1869.

Now let x_0 denote an irrational number such that $0 < x_0 < 1$. Let a_1 be the greatest natural number such that $x_0 < \frac{1}{a_1}$. Let $x_1 = \frac{1}{a_1} - x_0$. We then have $0 < x_1 < 1$. We proceed similarly with x_1 in place of x_0 and obtain the greatest natural number a_2 such that $x_1 < \frac{1}{a_2}$. We put $x_2 = \frac{1}{a_2} - x_1$ and so on. Thus we obtain an infinite sequence of natural numbers $a_1, a_2 \ldots$ and an infinite sequence of irrational numbers $x_1, x_2, \ldots$ such that $0 < x_n < 1$ for $n = 0, 1, 2, \ldots$ and $x_n = \frac{1}{a_n} - x_{n-1}$ for $n = 1, 2, \ldots$

Moreover, $\dfrac{1}{a_n+1} < x_{n-1} < \dfrac{1}{a_n}$ for $n = 1, 2, \ldots$ Hence $-x_{n-1} < -\dfrac{1}{a_n+1}$ and so

$$\frac{1}{a_{n+1}+1} < x_n < \frac{1}{a_n} - x_{n-1} < \frac{1}{a_n} - \frac{1}{a_n+1} = \frac{1}{a_n(a_n+1)}.$$

It follows that $a_{n+1}+1 > a_n(a_n+1)$ and so $a_{n+1} \geqslant a_n(a_n+1)$ for $n = 1, 2, \ldots$ From this, by induction, we easily infer that $a_{n+2} > 2^{2^n}$ for $n = 1, 2, \ldots$ Numbers a_n increase rapidly to infinity with n. It follows from the definition of numbers a_n and x_n ($n = 1, 2, \ldots$) that

$$x_0 = \frac{1}{a_1} - \frac{1}{a_2} + \frac{1}{a_3} - \ldots + \frac{(-1)^{n-1}}{a_n} + (-1)^n x_n. \tag{25}$$

Since $0 < x_n < \dfrac{1}{a_{n+1}}$, in view of the fact that $\lim\limits_{n\to\infty} a_{n+1} = +\infty$, we have $\lim\limits_{n\to\infty} x_n = 0$. Therefore formula (25) gives us an expansion of the irrational number x_0 into an infinite rapidly convergent series

$$x_0 = \frac{1}{a_1} - \frac{1}{a_2} + \frac{1}{a_3} - \frac{1}{a_4} + \ldots \tag{26}$$

where a_n ($n = 1, 2, \ldots$) are natural numbers satisfying the inequalities

$$a_{n+1} \geqslant a_n(a_n+1) \quad \text{for} \quad n = 1, 2, \ldots \tag{27}$$

We have thus proved that any irrational number x_0, $0 < x_0 < 1$, may be expressed in form (26).

It can be proved that every irrational number between 0 and 1 has precisely one representation of this form and that, a real number x_0 which can be expressed in form (26), where a_n ($n = 1, 2, \ldots$) are natural numbers satisfying conditions (27), is an irrational number (Sierpiński [4]).

CHAPTER VIII

CONTINUED FRACTIONS

1. Continued fractions and their convergents

Simple continued fractions have already been considered in connection with the Euclidean algorithm in § 9, Chapter I. We also gave there a method of developing a rational number into a simple continued fraction. Now we are going to consider slightly more general continued fractions of the form

$$a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \dots + \frac{1|}{|a_n}, \tag{1}$$

where n is a given natural number, a_0 a real number and $a_1, a_2, \dots, a_n$ positive numbers.

The number

$$R_k = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \dots + \frac{1|}{|a_k}, \tag{2}$$

where $k = 1, 2, \dots, n$, is called the kth *convergent* to the fraction (1). We define the 0th convergent as the number $R_0 = a_0$.

It follows from (2) that the kth convergent R_k is a function of $k+1$ variables, $a_0, a_1, \dots, a_k$, and that if for $k < n$ number a_k is replaced by number $a_k + \dfrac{1}{a_{k+1}}$, the convergent R_k turns into the convergent R_{k+1}.

Let

$$\begin{aligned} P_0 &= a_0, & Q_0 &= 1, \\ P_1 &= a_0 a_1 + 1, & Q_1 &= a_1, \\ P_k &= P_{k-1} a_k + P_{k-2}, & Q_k &= Q_{k-1} a_k + Q_{k-2} \\ & & &\text{for} \quad k = 2, 3, \dots, n. \end{aligned} \tag{3}$$

As is shown by an easy induction, P_k is a function of the variables $a_0, a_1, \dots, a_k$, Q_k being a function of $a_1, a_2, \dots, a_k$. Moreover, P_k and Q_k are integral polynomials of the variables in question. An immediate verification gives

$$\frac{P_0}{Q_0} = \frac{a_0}{1} = R_0, \quad \frac{P_1}{Q_1} = \frac{a_0 a_1 + 1}{a_1} = a_0 + \frac{1}{a_1} = R_1.$$

We prove that for any positive numbers $a_1, a_2, \dots, a_n$ the relation

$$P_k/Q_k = R_k, \quad k = 0, 1, 2, \dots, n, \tag{4}$$

holds.

As we have just seen, the relation is valid for $k = 0$ and $k = 1$. For $k = 2$ its validity follows from (3); we have

$$\frac{P_2}{Q_2} = \frac{P_1 a_2 + P_0}{Q_1 a_2 + Q_0} = \frac{(a_0 a_1 + 1) a_2 + a_0}{a_1 a_2 + 1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = R_2.$$

Suppose that (4) holds for $k = m$, where $2 \leqslant m < n$. Then for any positive numbers $a_1, a_2, \dots, a_m$ we have $R_m = P_m/Q_m$. By (3), the equality

$$R_m = \frac{P_{m-1} a_m + P_{m-2}}{Q_{m-1} a_m + Q_{m-1}} \tag{5}$$

holds for any positive numbers $a_1, a_2, \dots, a_m$. Equality (5) remains valid if a_m is replaced by $a_m + \dfrac{1}{a_{m+1}}$ on each side of the equality (since $a_{m+1} > 0$). But then R_m turns into R_{m+1} and, since on the right-hand side of the equality P_{m-1}, P_{m-2}, Q_{m-1}, Q_{m-2} do not depend on a_m, we have

$$R_{m+1} = \frac{P_{m-1}\left(a_m + \dfrac{1}{a_{m+1}}\right) + P_{m-2}}{Q_{m-1}\left(a_m + \dfrac{1}{a_{m+1}}\right) + Q_{m-2}} = \frac{(P_{m-1} a_m + P_{m-2}) a_{m+1} + P_{m-1}}{(Q_{m-1} a_m + Q_{m-2}) a_{m+1} + Q_{m-1}}.$$

Consequently, by (3),

$$R_{m+1} = \frac{P_m a_{m+1} + P_{m-1}}{Q_m a_{m+1} + Q_{m-1}} = \frac{P_{m+1}}{Q_{m+1}},$$

which shows the validity of (4) for $k = m+1$, and so, by induction, for any $k = 0, 1, 2, \dots, n$.

We now write

$$\Delta_k = P_{k-1} Q_k - Q_{k-1} P_k, \quad k = 1, 2, \dots, n.$$

We then have

$$\Delta_1 = P_0 Q_1 - Q_0 P_1 = a_0 a_1 - (a_0 a_1 + 1) = -1.$$

But, by (3),

$$\begin{aligned} \Delta_k &= P_{k-1}(Q_{k-1} a_k + Q_{k-2}) - Q_{k-1}(P_{k-1} a_k + P_{k-2}) \\ &= P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2} = -\Delta_{k-1} \quad \text{for} \quad k = 2, 3, \dots, n, \end{aligned}$$

whence, immediately, $\Delta_k = (-1)^k$ for $k = 1, 2, \dots, n$. We have thus proved

$$\Delta_k = P_{k-1} Q_k - Q_{k-1} P_k = (-1)^k \quad \text{for} \quad k = 1, 2, \dots, n. \tag{6}$$

2. Representation of irrational numbers by continued fractions

Let x denote an irrational number. Let $a_0 = [x]$. Since x is irrational, $0 < x - a_0 < 1$ which implies that number $x_1 = 1/(x - a_0)$ is an irrational number > 1. We set $a_1 = [x_1]$. Clearly, $[x_1]$ is a natural number and a reasoning similar to the above shows that number $x_2 = 1/(x_1 - a_1)$ is an irrational number > 1. Proceeding in this way, we obtain an infinite sequence $x_1, x_2, \dots$ of irrational numbers each greater than 1 and a sequence of natural numbers $a_n = [x_n]$ such that $x_n = 1/(x_{n-1} - a_{n-1})$ for any $n = 1, 2, \dots$; x_0 being taken as x. We then have

$$x_{n-1} = a_{n-1} + \frac{1}{x_n} \quad \text{for} \quad n = 1, 2, \dots$$

The sequence of the equalities

$$x = a_0 + \frac{1}{x_1}, \quad x_1 = a_1 + \frac{1}{x_2}, \quad \dots, \quad x_{n-1} = a_{n-1} + \frac{1}{x_n}$$

gives

$$x = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \dots + \frac{1|}{|a_{n-1}} + \frac{1|}{|x_n}. \tag{7}$$

Let

$$R_n = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \dots + \frac{1|}{|a_n}. \tag{8}$$

Comparing (7) and (8), we see that, if a_n in (8) is replaced by x_n, R_n turns into x.

P_k and Q_k being defined by (3), for an arbitrary a_0 and positive $a_1, a_2, \dots, a_n$ we have

$$R_n = \frac{P_n}{Q_n} = \frac{P_{n-1} a_n + P_{n-2}}{Q_{n-1} a_n + Q_{n-2}}.$$

Moreover, since P_{n-1}, P_{n-2}, Q_{n-1} and Q_{n-2} do not depend on a_n, by replacing a_n by x_n on each side of the above equality we obtain

$$x = \frac{P_{n-1} x_n + P_{n-2}}{Q_{n-1} x_n + Q_{n-2}}. \tag{9}$$

This formula is valid for any natural number $n > 1$; consequently, if we replace in it n by $n+1$, we get

$$x = \frac{P_n x_{n+1} + P_{n-1}}{Q_n x_{n+1} + Q_{n-1}},$$

whence, by (6),

$$(10) \qquad x - R_n = \frac{P_n x_{n+1} + P_{n-1}}{Q_n x_{n+1} + Q_{n-1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{(Q_n x_{n+1} + Q_{n-1}) Q_n}.$$

This and the inequality $x_{n+1} > a_{n+1}$ give together the following evaluation:

$$(11) \qquad |x - R_n| < \frac{1}{(Q_n a_{n+1} + Q_{n-1}) Q_n} = \frac{1}{Q_{n+1} Q_n}.$$

We are going to prove that $Q_k \geqslant k$ for any $k = 1, 2, \ldots$ Trivially this is true for $k = 1$ because $Q_1 = a_1$ is a natural number. If for a natural number k the inequality $Q_k \geqslant k$ holds, then, by (3), Q_k $(k = 0, 1, 2, \ldots)$ is a natural number and we have $Q_{k+1} = Q_k a_{k+1} + Q_{k-1} \geqslant Q_k + 1 \geqslant k+1$. Thus. by induction, the inequality $Q_k \geqslant k$ is proved for all $k = 1, 2, \ldots$ By (11) we then have

$$|x - R_n| < \frac{1}{n(n+1)} \quad \text{for} \quad n = 1, 2, \ldots$$

Hence $x = \lim\limits_{n \to \infty} R_n$. We express this by saying that number x is represented by the (infinite) simple continued fraction

$$(12) \qquad x = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \frac{1|}{|a_3} + \ldots$$

We have thus proved that *any irrational number x may be expressed as an infinite simple continued fraction, the representation being obtained by the use of the algorithm presented above.*

Since $a_{n+1} = [x_{n+1}] > x_{n+1} - 1$ and consequently $x_{n+1} < a_{n+1} + 1$, formula (10) implies

$$(13) \qquad |x - R_n| = \frac{1}{(Q_n x_{n+1} + Q_{n-1}) Q_n} > \frac{1}{(Q_n(a_{n+1} + 1) + Q_{n-1}) Q_n}$$
$$= \frac{1}{Q_n(Q_{n+1} + Q_n)}.$$

But, since $a_{n+2} \geqslant 1$, by replacing n by $n+1$ in (11) we obtain

$$(14) \qquad |x-R_{n+1}| < \frac{1}{(Q_{n+1}+Q_n)\,Q_{n+1}}.$$

The relation $Q_{n+1} = Q_n a_n + Q_{n-1} > Q_n$ applied to (13) and (14) gives the evaluation

$$(15) \qquad |x-R_{n+1}| < |x-R_n|, \qquad \text{valid for any } n = 1, 2, 3, \ldots$$

This means that of any two consecutive convergents to x, the second gives a better approximation than the first. Formula (10) shows that

$$x-R_n \begin{cases} > 0 & \text{for even } n, \\ < 0 & \text{for odd } n, \end{cases}$$

which means that *the even convergents are less than* x, *whereas the odd ones are greater than* x. This, combined with inequality (15), indicates that the even convergents increase strictly as they tend to x, while the odd convergents decrease strictly.

Now let a_0 denote an arbitrary integer and $a_1, a_2, \ldots$ an arbitrary infinite sequence of natural numbers. Applying the above-mentioned argument slightly modified, we conclude that if numbers R_k are defined by (2), then for any natural numbers n, $m > n$, we have

$$|R_m - R_n| < \frac{1}{n(n+1)}.$$

This proves that the infinite sequence R_n ($n = 1, 2, \ldots$) is convergent, i.e. that there exists a limit $x = \lim\limits_{n\to\infty} R_n$. We then write formula (12). Thus any infinite continued fraction (12) (where $a_1, a_2, \ldots$ are any natural numbers) represents a real number. Now, assuming (12), we write

$$(16) \qquad x_n = a_n + \frac{1|}{|a_{n+1}} + \frac{1|}{|a_{n+2}} + \ldots \qquad \text{for} \quad n = 0, 1, 2, \ldots,$$

where $x_0 = x$. Let

$$(17) \qquad R_k^{(n)} = a_n + \frac{1|}{|a_{n+1}} + \ldots + \frac{1|}{|a_{n+k}} \qquad \text{for} \quad k = 1, 2, \ldots$$

Then

$$(18) \qquad \lim_{k\to\infty} R_{k+1}^{(n)} = x_n \qquad \text{and} \qquad \lim_{k\to\infty} R_k^{(n+1)} = x_{n+1}.$$

But, clearly,

$$R_{k+1}^{(n)} = a_n + \frac{1}{R_k^{(n+1)}}$$

whence, by (18)

$$(19) \qquad x_n = a_n + \frac{1}{x_{n+1}} \quad \text{for} \quad n = 0, 1, 2, \ldots$$

We also have

$$R_{k+2}^{(n)} = a_n + \frac{1}{R_{k+1}^{(n+1)}} = a_n + \cfrac{1}{a_{n+1} + \cfrac{1}{R_k^{(n+2)}}},$$

but, since $R_k^{(n+2)} \geqslant a_{n+2}$, we have

$$R_{k+2}^{(n)} \geqslant a_n + \cfrac{1}{a_{n+1} + \cfrac{1}{a_{n+2}}},$$

whence, in virtue of $\lim\limits_{k\to\infty} R_{k+2}^{(n)} = x_n$, we infer

$$x_n \geqslant a_n + \cfrac{1}{a_{n+1} + \cfrac{1}{a_{n+2}}}.$$

Consequently $x_n > a_n$ for any $n = 0, 1, 2, \ldots$ Therefore $x_{n+1} > a_{n+1}$ and so $x_{n+1} > 1$ for $n = 1, 2, \ldots$ On the other hand, by (19) we have $x_n < a_n + 1$. Thus we see that $a_n < x_n < a_n + 1$ for $n = 0, 1, 2, \ldots$, whence $a_n = [x_n]$ for $n = 0, 1, 2, \ldots$ This, by (19), shows that if (12) is any representation of x as an infinite simple continued fraction, then the relations

$$(20) \qquad \begin{gathered} x_1 = \frac{1}{x - a_0}, \quad x_{n+1} = \frac{1}{x_n - a_n} \quad \text{for} \quad n = 1, 2, \ldots, \\ a_n = [x_n] \quad \text{for} \quad n = 0, 1, 2, \ldots \end{gathered}$$

hold. This proves that any irrational number is uniquely expressible as an infinite simple continued fraction.

We now prove that any infinite simple continued fraction represents an irrational number. Accordingly we suppose that a rational number

$x = l/m$ (with $(l, m) = 1$) is expressed as in (12). As we have just seen, (12) implies formulae (20). Therefore

$$a_0 = \left[\frac{l}{m}\right], \quad x_1 = \frac{1}{\dfrac{l}{m} - \left[\dfrac{l}{m}\right]} = \frac{m}{l - m\left[\dfrac{l}{m}\right]}.$$

But

$$\left[\frac{l}{m}\right] > \frac{l}{m} - 1, \quad \text{whence} \quad l - m\left[\frac{l}{m}\right] < l - m\left(\frac{l}{m} - 1\right) = m.$$

Consequently, if $x_1 = l_1/m_1$, l_1/m_1 being an irreducible fraction, then $m_1 < m$. Thus we come to the conclusion that the denominators of the rational numbers $x_0, x_1, x_2, \ldots$ decrease strictly, which is impossible. This proves that a rational number cannot be expressed as an infinite simple continued fraction.

We sum up our conclusions in

THEOREM 1. *Every irrational number can be expressed in exactly one way as an infinite simple continued fraction* (12) (*where a_0 is an integer and $a_1, a_2, \ldots$ are natural numbers defined by formulae* (20)). *Conversely, any infinite simple continued fraction represents an irrational number.*

For irrational numbers of the 2nd degree representations as simple continued fractions are known. (We shall discuss this in detail in § 4.) Among other irrational numbers there are very few for which representations as continued fractions are known. Number e belongs to this class. It has been proved that

$$e = 2 + \frac{1|}{|1} + \frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|4} + \frac{1|}{|1} + \ldots + \frac{1|}{|1} + \frac{1|}{|2k} + \frac{1|}{|1} + \ldots$$

We also have

$$\frac{e^2 - 1}{e^2 + 1} = \frac{1|}{|1} + \frac{1|}{|3} + \frac{1|}{|5} + \frac{1|}{|7} + \ldots$$

The rule according to which the numbers appear in the sequence $a_0, a_1, a_2, \ldots$ of quotients of the simple continued fraction which expresses number e^2 is also known. Here we have

$$7,\ 2,\ 1,\ 1,\ 3,\ 18,\ 5,\ 1,\ 1,\ 6,\ 30, \ldots, 2 + 3k,\ 1,\ 1,\ 3 + 3k,\ 18 + 12k, \ldots$$

No such rule is known for the sequence of quotients $a_0, a_1, a_2, \ldots$ of the simple continued fraction for the number π. G. Lochs [1] has calculated the numbers a_k for $k = 0, 1, \ldots, 968$. The greatest of them is the number $a_{431} = 20776$; all natural numbers $\leqslant 34$ appear among the a_k's and number 1 appears 393 times. Here are the first 30 of the quotients: 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4.

R. W. Gasper Jr. [1] has calculated a_k for $k \leqslant 204103$. The largest is $a_{156381} = 179136$.

It is easy to find a sufficient and necessary condition for a non-integral number x which ensures that in the representation of x as a simple continued fraction the first quotient a_1 is equal to a given natural number m. In fact, we have $a_1 = [x_1] = \left[\dfrac{1}{x-a_0}\right]$; therefore in order that $a_1 = m$ it is necessary and sufficient that $m \leqslant 1/(x-a_0) < m+1$, i.e.

$$a_0 + \frac{1}{m+1} < x \leqslant a_0 + \frac{1}{m}.$$

In particular, the condition for a number x with $0 < x < 1$ to have the first quotient equal to m in the representation of x as a continued fraction is

$$\frac{1}{m+1} < x \leqslant \frac{1}{m}.$$

Consequently, number x must be in an interval whose length is $1/m - 1/(m+1) = 1/\big(m(m+1)\big)$. From this we infer that the probability of the event that the first quotient of the representation of a real number x as a continued fraction is equal to m is $1/\big(m(m+1)\big)$. Consequently, for $m = 1$ the probability is equal to $\frac{1}{2}$, for $m = 2$ it is $\frac{1}{6}$, for $m = 3$ it is only $\frac{1}{12}$, and so on. We see that the probability decreases as m tends to infinity. It is easy to verify that the probability of the event that the first quotient is > 10 is equal to $\frac{1}{11}$. This is the reason why in general the first quotient a_1 is a comparatively small number.

A more difficult task is to calculate the probability of the event that the second quotient is equal to a given natural number m. (The probability that the kth digit in the representation of a real number as a decimal is equal to a given digit c is equal to $\frac{1}{10}$ for any k and any digit c.)

The theory of measure provides methods on the basis of which one can prove that the probability of the event that among the quotients of the representation of an irrational number as a simple continued fraction there are finitely many (or zero) quotients equal to 1 is zero. (Cf. Hausdorff [1], p. 426.) Similarly, the probability that among the quotients there are only finitely many different numbers is zero.

3. Law of the best approximation

Now we are going to prove a theorem which shows the importance of the theory of continued fractions in finding approximate values of irrational numbers.

Let x be a given irrational number that is represented as a continued fraction as in (12), and let r/s be a rational number that approximates x better than the nth convergent R_n of x. In other words, we suppose that

$$\left|x-\frac{r}{s}\right| < |x-R_n|. \tag{21}$$

In virtue of (15) we have $|x-R_n| < |x-R_{n-1}|$, whence, by (21), we get

$$\left|x-\frac{r}{s}\right| < |x-R_{n-1}|. \tag{22}$$

But, as we have already learned, number x lies between numbers R_{n-1} and R_n. Hence inequalities (21) and (22) prove that number r/s also lies between numbers R_{n-1} and R_n. Therefore we have

$$\left|\frac{r}{s}-R_{n-1}\right| < |R_{n-1}-R_n|. \tag{23}$$

But, by (4) and (6),

$$|R_{n-1}-R_n| = \left|\frac{P_{n-1}}{Q_{n-1}}-\frac{P_n}{Q_n}\right| = \frac{|P_{n-1}\,Q_n-Q_{n-1}\,P_n|}{Q_{n-1}\,Q_n} = \frac{1}{Q_{n-1}\,Q_n},$$

which, in view of (23), gives

$$\frac{|rQ_{n-1}-sP_{n-1}|}{sQ_{n-1}} < \frac{1}{Q_{n-1}\,Q_n}. \tag{24}$$

Number $rQ_{n-1}-sP_{n-1}$ is an integer and it cannot be equal to zero, because, if it were, $r/s = R_{n-1}$, contrary to inequality (22). Thus we have proved that $|rQ_{n-1}-sP_{n-1}| > 1$; this and (24) show that $s > Q_n$. We have thus proved the following

THEOREM 2. *Suppose that a rational number r/s, being an integer and s a natural number, provides an approximation of an irrational number x better than the n-th convergent R_n ($n \geqslant 1$) of x. Then the denominator s of the rational number r/s is greater than the denominator of the convergent R_n.*

This theorem is known as the *law of the best approximation.*

For example, representing π as simple continued fraction we see that its second convergent is $\frac{22}{7}$; therefore the rational $\frac{22}{7}$ approximates number π better than any other rational with a denominator $\leqslant 7$. Similarly, since the third convergent is 355/113, this number approximates π better than any rational with a denominator $\leqslant 113$.

4. Continued fractions of quadratic irrationals

Let D be a natural number which is not a square of a natural number. We apply to it the algorithm presented in § 2 and obtain the representation of the irrational number $x = \sqrt{D}$ as a simple continued fraction. We have

$$a_0 = [\sqrt{D}], \qquad \sqrt{D} = a_0 + \frac{1}{x_1}; \tag{25}$$

therefore

$$x_1 = \frac{1}{\sqrt{D} - a_0} = \frac{\sqrt{D}+a_0}{D-a_0^2} = \frac{\sqrt{D}+b_1}{c_1},$$

where $b_1 = a_0$, $c_1 = D-a_0^2$ and $c_1 > 0$ (because $a_0 = [\sqrt{D}] < \sqrt{D}$, and D is not the square of a natural number). We thus obtain

$$D-b_1^2 = c_1. \tag{26}$$

Further, we have $a_1 = [x_1]$ and $x_1 = a_1 + \dfrac{1}{x_2}$, whence, by (26),

$$x_2 = \frac{1}{x_1-a_1} = \frac{1}{\dfrac{\sqrt{D}+b_1}{c_1} - a_1} = \frac{c_1}{\sqrt{D}+b_1-a_1 c_1} = \frac{c_1(\sqrt{D}+a_1 c_1-b_1)}{D-(a_1 c_1-b_1)^2}$$

$$= \frac{c_1(\sqrt{D}+a_1 c_1-b_1)}{D-b_1^2-a_1^2 c_1^2+2a_1 b_1 c_1} = \frac{\sqrt{D}+a_1 c_1-b_1}{1-a_1^2 c_1+2a_1 b_1} = \frac{\sqrt{D}+b_2}{c_2},$$

where $b_2 = a_1 c_1 - b_1$ and $c_2 = 1-a_1^2 c_1+2a_1 b_1$.

For natural numbers $n > 1$ we write

$$b_{n+1} = a_n c_n - b_n, \qquad c_{n+1} = c_{n-1} - a_n^2 c_n + 2a_n b_n. \tag{27}$$

We are going to prove that for $n > 1$ the equality

$$D-b_n^2 = c_{n-1} c_n \tag{28}$$

holds.

In fact,

$$D-b_2^2 = D-(a_1c_1-b_1)^2 = D-b_1^2-a_1^2c_1^2+2a_1b_1c_1$$
$$= c_1-a_1^2c_1^2+2a_1b_1c_1 = c_1(1-a_1^2c_1+2a_1b_1) = c_1c_2.$$

If for a natural number $n > 1$ we have $D-b_n^2 = c_{n-1}c_n$, then, by (27),

$$D-b_{n+1}^2 = D-(a_nc_n-b_n)^2 = D-b_n^2-a_n^2c_n^2+2a_nb_nc_n$$
$$= c_{n-1}c_n-a_n^2c_n^2+2a_nb_nc_n = c_n(c_{n-1}-a_n^2c_n+2a_nb_n)$$
$$= c_nc_{n+1},$$

which, by induction, gives formula (28). The assumption regarding D ensures, by (28), that $c_n \neq 0$ for any $n = 1, 2, \ldots$

We now prove that

$$x_n = \frac{\sqrt{D}+b_n}{c_n} \quad \text{for} \quad n = 1, 2, \ldots \tag{29}$$

As has just been shown, formula (29) holds for $n = 1$ and $n = 2$. Suppose that it is true for a natural number $n > 1$. Then, by (27) and (28),

$$x_{n+1} = \frac{1}{x_n-a_n} = \frac{1}{\dfrac{\sqrt{D}+b_n}{c_n}-a_n} = \frac{c_n}{\sqrt{D}+b_n-a_nc_n}$$
$$= \frac{c_n(\sqrt{D}+a_nc_n-b_n)}{D-(a_nc_n-b_n)^2} = \frac{\sqrt{D}+b_{n+1}}{c_{n+1}}$$

and thus formula (29) follows by induction.

As we know c_1 is a natural number; so in view of $b_1 = a_0 = [\sqrt{D}] < \sqrt{D}$ and thus $0 < \sqrt{D}-b_1 < 1$, we have $0 < (\sqrt{D}-b_1)/c_1 < 1$ and, since $x_1 > 1$, we have $(\sqrt{D}+b_1)/c_1 > 1$.

Thus we see that

$$0 < \frac{\sqrt{D}-b_1}{c_1} < 1 < \frac{\sqrt{D}+b_1}{c_1}.$$

We are going to prove that the above formula is valid for any natural number n, i.e. that

$$0 < \frac{\sqrt{D}-b_n}{c_n} < 1 < \frac{\sqrt{D}+b_n}{c_n} \tag{30}$$

holds for any natural number n.

The formula is true for $n = 1$. Suppose that it is true for an arbitrary natural number n. By (29) we have

$$\frac{\sqrt{D}+b_{n+1}}{c_{n+1}} = x_{n+1} > 1.$$

By (27) and (28)

$$\frac{\sqrt{D}-b_{n+1}}{c_{n+1}} = \frac{D-b_{n+1}^2}{c_{n+1}(\sqrt{D}+b_{n+1})} = \frac{c_n}{\sqrt{D}+b_{n+1}} = \frac{c_n}{\sqrt{D}+a_n c_n - b_n}$$

$$= \frac{1}{\dfrac{\sqrt{D}-b_n}{c_n}+a_n},$$

whence

$$0 < \frac{\sqrt{D}-b_{n+1}}{c_{n+1}} < 1,$$

because in virtue of (30)

$$\frac{\sqrt{D}-b_n}{c_n} + a_n > a_n \geqslant 1.$$

Thus inequalities (30) are proved by induction.

If $c_n < 0$ for a natural number n, then, by (30), we have $\sqrt{D}-b_n < 0$ and $\sqrt{D}+b_n < 0$, whence $2\sqrt{D} < 0$, which is impossible. Therefore $c_n > 0$ for all $n = 1, 2, \ldots$ Consequently $\sqrt{D}-b_n < c_n < \sqrt{D}+b_n$, whence $\sqrt{D}-b_n < \sqrt{D}+b_n$ and so $b_n > 0$ for $n = 1, 2, \ldots$ Consequently, (30) implies that $b_n < \sqrt{D}$ and $c_n < \sqrt{D}+b_n < 2\sqrt{D}$.

From this we infer that the number of different systems of natural numbers b_n and c_n is less than $2D$. Therefore among the terms of the infinite sequence (29), for $n = 1, 2, \ldots$ there are only finitely many different numbers, each of them being less than $2D$. This implies that among the numbers $x_1, x_2, \ldots, x_{2D}$ at least two are equal. Consequently, there exist numbers k and $s < 2D$ such that

$$x_k = x_{k+s}; \tag{31}$$

since

$$x_{n+1} = \frac{1}{x_n - [x_n]} \quad \text{for} \quad n = 1, 2, \ldots,$$

(31) gives $x_{k+1} = x_{k+s+1}$ and, more generally, $x_n = x_{n+s}$ for $n \geqslant k$.

Therefore the infinite sequence $x_1, x_2, \ldots$ and consequently the sequence $a_1, a_2, \ldots$ (a_n being equal to $[x_n]$, $n = 1, 2, \ldots$) is periodic.

Let

$$x'_n = \frac{\sqrt{D}-b_n}{c_n} \quad \text{for} \quad n = 1, 2, \ldots \tag{32}$$

It follows from (29) that, if we change the sign at $\sqrt{D}$, number x'_n turns into $-x'_n$ and, consequently, the equality $x_n = a_n + 1/x_{n+1}$ turns into $-x'_n = a_n - 1/x'_{n+1}$, i.e. into the equality $1/x'_{n+1} = a_n + x'_n$. Since, by (32) and (30), $0 < x'_n < 1$, we obtain

$$a_n = \left[\frac{1}{x'_{n+1}}\right] \quad \text{for} \quad n = 1, 2, \ldots \tag{33}$$

Furthermore, since equality (31) gives $x'_k = x'_{k+s}$, we see that, by (33), for $k > 1$ we have

$$a_{k-1} = \left[\frac{1}{x'_k}\right] = \left[\frac{1}{x'_{k+s}}\right] = a_{k+s-1}.$$

Therefore, in virtue of the relation $x_n = a_n + 1/x_{n+1}$ and (31), we infer that $x_{k-1} = x_{k+s-1}$.

Repeating the above argument for $k > 2$, we obtain $x_{k-2} = x_{k+s-2}$ and so on. This shows that the sequence $x_1, x_2, \ldots$ and, consequently, the sequence $a_1, a_2, \ldots$ have a pure period, i.e. a period which begins at the first term (at a_1 not at a_0).

Thus we have proved

$$x_{n+s} = x_n \quad \text{and} \quad a_{n+s} = a_n \quad \text{for} \quad n = 1, 2, \ldots \tag{34}$$

The sequences of the formulae

$$x_1 = a_1 + \frac{1}{x_2}, \quad x_2 = a_2 + \frac{1}{x_3}, \quad \ldots, \quad x_s = a_s + \frac{1}{x_{s+1}} = a_s + \frac{1}{x_1}$$

and

$$-x'_1 = a_1 - \frac{1}{x'_2}, \quad -x'_2 = a_2 - \frac{1}{x'_3}, \quad \ldots, \quad -x'_s = a_s - \frac{1}{x'_{s+1}} = a_s - \frac{1}{x'_1}$$

or, equivalently,

$$\frac{1}{x'_2} = a_1 + \frac{1}{\left(\frac{1}{x'_1}\right)}, \quad \frac{1}{x'_3} = a_2 + \frac{1}{\left(\frac{1}{x'_2}\right)}, \quad \ldots, \quad \frac{1}{x'_1} = a_s + \frac{1}{\left(\frac{1}{x'_s}\right)}$$

have as their immediate consequence the formulae

$$(35)\qquad \begin{aligned} x_1 &= a_1 + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_s} + \frac{1|}{|x_1}, \\ \frac{1}{x_1'} &= a_s + \frac{1\;|}{|a_{s-1}} + \ldots + \frac{1|}{|a_1} + \frac{1\;\;|}{\left|\left(\frac{1}{x_1'}\right)\right.}. \end{aligned}$$

But, in virtue of (25), $\sqrt{D} = a_0 + 1/x_1$ and $-\sqrt{D} = a_0 - 1/x_1'$, whence $\sqrt{D} = -a_0 + 1/x_1'$. Therefore formulae (35) imply the relations

$$\begin{aligned} \sqrt{D} &= a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_s} + \frac{1|}{|x_1}, \\ \sqrt{D} &= a_s - a_0 + \frac{1\;|}{|a_{s-1}} + \frac{1\;|}{|a_{s-2}} + \ldots + \frac{1|}{|a_1} + \frac{1\;\;|}{\left|\left(\frac{1}{x_1'}\right)\right.}. \end{aligned}$$

Since $x_1 > 1$ and $1/x_1' > 1$, these relations give

$$(36)\ a_s = 2\left[\sqrt{D}\right], \qquad a_1 = a_{s-1}, \qquad a_2 = a_{s-2}, \qquad \ldots, \qquad a_{s-1} = a_1.$$

Thus we see that the sequence $a_1, a_2, \ldots, a_{s-1}$ is symmetric.

We may up the conclusions just obtained in the following

THEOREM 3. *If D is a natural number which is not the square of a natural number, then in the representation of $\sqrt{D}$ as a simple continued fraction,*

$$\sqrt{D} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots,$$

the sequence $a_1, a_2, \ldots$ is periodic. Moreover, the period of the sequence is pure and, if it consists of s terms $a_1, a_2, \ldots, a_s$, then $s < 2D$, $a_s = 2\left[\sqrt{D}\right]$ and the sequence $a_1, a_2, \ldots, a_{s-1}$ is symmetric.

The representation of $\sqrt{D}$ as a continued fraction is usually written in the form $\sqrt{D} = (a_0\,; \overline{a_1, a_2, \ldots, a_s})$, the bar above the terms indicating that they form a period.

It is not true, however, that the square roots of natural numbers which are not squares are the only quadratic irrationals that possess the properties listed in Theorem 3.

It can be proved that the class of positive irrational numbers which have these properties coincides with the class of the square roots of rationals greater than 1.

For example, as is easy to check,

$$\sqrt{\frac{13}{2}} = (2;\overline{1,1,4}), \qquad \sqrt{\frac{5}{3}} = (1;\overline{3,2}),$$

$$\sqrt{\frac{26}{5}} = (2;\overline{3,1,1,3,4}).$$

Other quadratic irrationals do not have these properties; for example,

$$\frac{1+\sqrt{13}}{4} = (0;\overline{1,6,1,1,1}), \qquad \frac{2+\sqrt{19}}{5} = (0;\overline{1,3,1,2,8,2}),$$

$$\frac{1+\sqrt{365}}{14} = (1;\overline{2,3,2}), \qquad \sqrt{\frac{1}{2}} = (0;\overline{1,2}),$$

$$\frac{1+\sqrt{17}}{2} = (2;\overline{1,1,2}).$$

Now we are going to present a practical method˙ of finding the representation of the number $\sqrt{D}$ as a continued fraction. To this aim, we prove the following

LEMMA. *If k is a natural number and x a real number, then*

$$\left[\frac{x}{k}\right] = \left[\frac{[x]}{k}\right]. \tag{37}$$

PROOF. Since $[x] \leqslant x$, we have

$$\frac{[x]}{k} \leqslant \frac{x}{k}, \quad \text{whence} \quad \left[\frac{[x]}{k}\right] \leqslant \left[\frac{x}{k}\right].$$

To prove the converse inequality we use the inequality $t-[t] < 1$ for $t = \frac{[x]}{k}$. We have

$$\frac{[x]}{k} - \left[\frac{[x]}{k}\right] < 1, \quad \text{whence} \quad [x] < k\left[\frac{[x]}{k}\right] + k$$

and, consequently, the numbers on both sides of the last inequality being integers, $[x] \leqslant k\left[\frac{[x]}{k}\right] + k - 1$.

In virtue of the relation $x < [x]+1$, we infer that

$$x < k\left[\frac{[x]}{k}\right]+k$$

and so $\left[\frac{x}{k}\right] < \left[\frac{[x]}{k}\right]+1$, whence $\left[\frac{x}{k}\right] \leqslant \left[\frac{[x]}{k}\right]$,

as was to be proved. This completes the proof of formula (37). □

In view of the lemma, by (29), we have

$$a_n = [x_n] = \left[\frac{\sqrt{D}+b_n}{c_n}\right] = \left[\frac{[\sqrt{D}]+b_n}{c_n}\right] = \left[\frac{a_0+b_n}{c_n}\right],$$

i.e.

$$a_n = \left[\frac{a_0+b_n}{c_n}\right] \quad \text{for} \quad n = 1, 2, \ldots \tag{38}$$

Hence, by (27) and (28), we obtain the following algorithm for representing the number $\sqrt{D}$ as a simple continued fraction:

We set $a_0 = [\sqrt{D}]$, $b_1 = a_0$, $c_1 = D-a_0^2$ *and we find the numbers* a_{n-1}, b_n, *and* c_n *successively using the formulae*

$$a_{n-1} = \left[\frac{a_0+b_{n-1}}{c_{n-1}}\right], \qquad b_n = a_{n-1}c_{n-1}-b_{n-1}, \qquad c_n = \frac{D-b_n^2}{c_{n-1}}.$$

Now we look at the sequence

$$(b_2, c_2), \quad (b_3, c_3), \quad (b_4, c_4), \quad \ldots$$

and find the smallest index s for which, say, $b_{s+1} = b_1$ *and* $c_{s+1} = c_1$; *the representation of* $\sqrt{D}$ *as a simple continued fraction is then*

$$\sqrt{D} = (a_0; \overline{a_1, a_2, \ldots, a_s}).$$

By this algorithm the representation of $\sqrt{D}$ as a simple continued fraction is obtained by finitely many rational operations on rational numbers.

REMARK. Since the period, the last term excluded (this, as we know, being $2[\sqrt{D}]$), is symmetric, the task of finding it reduces to finding at most half of its terms. Therefore it is of practical importance to know when half of the terms have already been found. It can be proved that *if the number s* *of the terms of the period is even, then number $\frac{1}{2}s$ is equal to the first index k for which $b_{k+1} = b_k$; if s is odd, then $\frac{1}{2}(s-1)$ is the first index k for which $c_{k+1} = c_k$*(¹).

EXAMPLES. We find the representation of number $\sqrt{a^2-2}$, where a is a natural number $\geqslant 3$, as a simple continued fraction. We have $(a-1)^2 = a^2-2a+1 < a^2-2 < a^2$. Therefore $a_0 = [\sqrt{a^2-2}] = a-1$. Hence

$$b_1 = a_0 = a-1,\ c_1 = D-a_0^2 = a^2-2-(a-1)^2 = 2a-3,$$

whence

$$a_1 = \left[\frac{a_0+b_1}{c_1}\right] = \left[\frac{2a-2}{2a-3}\right] = \left[1+\frac{1}{2a-3}\right] = 1$$

(since, by $a \geqslant 3$, we have $2a-3 \geqslant 3$). Hence, further,

$$b_2 = a_1 c_1 - b_1 = 2a-3-(a-1) = a-2,$$

$$c_2 = \frac{D-b_2^2}{c_1} = \frac{a^2-2-(a-2)^2}{2a-3} = \frac{4a-6}{2a-3} = 2,$$

$$a_2 = \left[\frac{a_0+b_2}{a_2}\right] = \left[\frac{a-1+a-2}{2}\right] = \left[a-\frac{3}{2}\right] = a-2,$$

whence

$$b_3 = a_2 c_2 - b_2 = (a-2)2-(a-2) = a-2,$$

$$c_3 = \frac{D-b_3^2}{c_2} = \frac{a^2-2-(a-2)^2}{2} = \frac{4a-6}{2} = 2a-3,$$

$$a_3 = \left[\frac{a_0+b_3}{c_3}\right] = \left[\frac{a-1+a-2}{2a-3}\right] = 1,$$

whence

$$b_4 = a_3 c_3 - b_3 = 2a-3-(a-2) = a-1,$$

$$c_4 = \frac{D-b_4^2}{c_3} = \frac{a^2-2-(a-1)^2}{2a-3} = 1,$$

$$a_4 = \left[\frac{a_0+b_4}{c_4}\right] = \frac{a-1+a-1}{1} = 2a-2.$$

(¹) This theorem is due to T. Muir; cf. Perron [1], p. 91.

Hence

$$b_5 = a_4 c_4 - b_4 = 2a-2-(a-1) = a-1 = b_1,$$

$$c_5 = \frac{D-b_5^2}{c_4} = \frac{a^2-2-(a-1)^2}{1} = 2a-3 = c_1.$$

Therefore $b_5 = b_1$ and $c_5 = c_1$, which implies that $s = 4$. The desired representation is then:

(39) $\sqrt{a^2-2} = (a-1;\overline{1, a-2, 1, 2a-2})$ for any natural $a \geqslant 3$.

The fact that the quotients a_1 and a_3 (and, more generally, a_n, n being odd) do not depend on a is worth noticing.

Formula (39) does not hold for $a = 2$. In fact, $\sqrt{2} = 1 + \dfrac{1}{1+\sqrt{2}}$ and so $\sqrt{2} = (1,\overline{2})$. Substituting 3, 4, 5 for a in (39), we obtain

$$\sqrt{7} = (2;\overline{1, 1, 1, 4}), \qquad \sqrt{14} = (3;\overline{1, 2, 1, 6}),$$
$$\sqrt{23} = (4;\overline{1, 3, 1, 8}).$$

The following representations are found in a similar way:

$\sqrt{a^2+1} = (a;\overline{a, 2a})$ for any natural number a;

$\sqrt{a^2-1} = (a-1;\overline{1, 2a-2})$, $\sqrt{a^2-a} = (a-1;\overline{2, 2a-2})$

for $a = 2, 3, \ldots$;

$\sqrt{a^2+4} = (a;\overline{\tfrac{1}{2}(a-1), 1, 1, \tfrac{1}{2}(a-1), 2a})$ for odd $a > 1$;

$\sqrt{a^2-4} = (a-1;\overline{1, \tfrac{1}{2}(a-3), 2, \tfrac{1}{2}(a-3), 1, 2a-2})$ for odd $a > 3$;

$\sqrt{4a^2+4} = (2a;\overline{a, 4a})$ for natural numbers a;

$\sqrt{(na)^2+a} = (na;\overline{2n, 2an})$, $\sqrt{(na)^2+2a} = (na;\overline{n, 2na})$ for natural numbers a, n;

$\sqrt{(na^2)^2-a} = (na-1;\overline{1, 2n-2, 1, 2(na-1})$ for natural numbers a and $n > 1$.

Now we find all natural numbers D for which the representation of $\sqrt{D}$ as a simple continued fraction has a period consisting of one term only.

It follows from property (36) of the representation of $\sqrt{D}$ as a simple continued fraction that in this case $\sqrt{D} = (a;\overline{2a})$, whence we easily infer that $\sqrt{D} = a + \dfrac{1}{a+\sqrt{D}}$, and so $D = a^2+1$. Thus we come to the following easy conclusion: *in order that for a natural number D the number $\sqrt{D}$ should have a representation as a simple continued fraction with a period consisting of one term only it is necessary and sufficient that $D = a^2+1$, where a is a natural number.*

It is also easy to find all natural numbers D for which the representation of $\sqrt{D}$ as a simple continued fraction has a period consisting of two terms. In fact, by (36), we have $\sqrt{D} = (a; \overline{b, 2a})$ where $b \neq 2a$. Hence $\sqrt{D} = a + \dfrac{1|}{|b} + \dfrac{1\ |}{|a+\sqrt{D}}$ and, consequently, $D = a^2 + \dfrac{2a}{b}$. It follows that $2a = kb$, where k is a natural number > 1 since $b \neq 2a$. Hence we conclude that *in order that for a natural number D the number $\sqrt{D}$ should have a representation as a simple continued fraction with a period consisting of two terms it is necessary and sufficient that $D = a^2+k$, where k is a divisor greater than* 1 *of number* $2a$.

Now we are going to find these natural numbers for which the period of the representation of $\sqrt{D}$ as a simple continued fraction consists of three terms.

Suppose that D is such a number. Then $\sqrt{D} = (a_0; \overline{a_1, a_2, 2a_0})$. Since, in view of Theorem 3, the sequence a_1, a_2 must be symmetric, we have $a_1 = a_2$ and, moreover, $a_1 \neq 2a_0$ since otherwise the period of the simple continued fraction for $\sqrt{D}$ would consist of one term a_1. This shows that the formula

$$\sqrt{D} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_1} + \frac{1\ \ |}{|a_0+\sqrt{D}} \tag{40}$$

holds. This ($\sqrt{D}$ being irrational) is clearly equivalent to the formula

$$D = a_0^2 + \frac{2a_0 a_1 + 1}{a_1^2+1}. \tag{41}$$

Hence it follows that in order that a natural number D should belong to the class under consideration it is necessary and sufficient that it should be of form (41). We are now going to show that a natural number D is of form (41) if and only if a_1 is an even number and

$$a_0 = (a_1^2+1)\,k + \tfrac{1}{2}a_1, \qquad \text{where} \qquad k = 1, 2, \ldots \tag{42}$$

The condition is sufficient. The argument is that if a_1 is an even natural number and (42) holds, then a_0 is a natural number, $2a_0 > a_1$ and

$$2a_0 a_1 + 1 = 2(a_1^2+1)a_1 k + a_1^2 + 1 = (a_1^2+1)(2a_1 k+1),$$

number D of (41) being natural.

On the other hand, if for some natural numbers a_0 and $a_1 \neq 2a_0$ number D of (41) is natural, then, since $2a_0 a_1 + 1$ is odd, number a_1^2+1 (as a divisor of it) must also be odd; so number a_1 is even and, since number D of (41) is an integer and, consequently, $\dfrac{2a_0 a_1+1}{a_1^2+1} - 1 = \dfrac{(a_0 - a_1/2)\,2a_1}{a_1^2+1}$ is an integer, number a_1^2+1 divides number $(a_0 - a_1/2)\,2a_1$. But $(2a_1, a_1^2+1) = 1$ (since a_1 is even); therefore number $a_0 - a_1/2$ is divisible by a_1^2+1 and this results in the equality $a_0 - a_1/2 = (a_1^2+1)k$, where k is an integer. This gives formula (42). But since $2a_0 \neq a_1$, we must have $k > 0$, and so k is a natural number. The necessity of the condition is thus proved.

THEOREM 4. *All natural numbers D for which the representation of the number $\sqrt{D}$ as a simple continued fraction has a period consisting of three terms are given by the formula*

$$D = ((a_1^2+1)k + a_1/2)^2 + 2a_1 k + 1,$$

where a_1 is an even natural number, $k = 1, 2, \ldots$ The representation is then of the form

$$\sqrt{D} = (a_0; \overline{a_1, a_1, 2a_0})\,(^1).$$

It is not difficult to prove that

$$D = ((a_1^2-1)k + a_1/2)^2 + (2a_1 k + 1)^2.$$

In particular, Theorem 4 implies that all the natural numbers D for which the simple continued fraction for $\sqrt{D}$ has a period consisting of three terms, the first two of them being equal to 2, are the numbers

$$D = (5k+1)^2 + 4k + 1, \qquad \text{where} \qquad k = 1, 2, \ldots$$

---

(1) As regards the generalization of this theorem to periods consisting of an arbitrary number of terms cf. Perron [1], I, p. 88, Satz 3, 17; cf. also ibid., pp. 89–90, Drittes Beispiel $k = 3$.

By using Theorem 4 it is easy to verify that among all the numbers $D \leqslant 1000$ there are only 7 numbers, such that $\sqrt{D}$ represented as simple continued fraction has a period consisting of three terms. They are the numbers 41, 130, 269, 370, 458, 697, 986.

THEOREM 5. *If s is a natural number and > 1, $a_1, a_2, \ldots, a_{s-1}$ is the symmetric part of the period of the simple continued fraction for $\sqrt{D_0}$, D_0 being a natural number, then there exist infinitely many natural numbers D for which $a_1, a_2, \ldots, a_{s-1}$ is the symmetric part of the period of the simple continued fraction for $\sqrt{D}$* (cf. Kraïtchik [1], pp. 57–58).

PROOF. If

$$\sqrt{D_0} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1\ |}{|a_{s-1}} + \frac{1\quad |}{|a_0 + \sqrt{D}},$$

then, if P_k/Q_k denotes the kth convergent of the fraction $\frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1\ |}{|a_{s-1}}$, we have

$$\sqrt{D_0} = a_0 + \frac{P_{s-1}(a_0 + \sqrt{D_0}) + P_{s-2}}{Q_{s-1}(a_0 + \sqrt{D_0}) + Q_{s-2}},$$

whence, since $\sqrt{D_0}$ is irrational,

$$Q_{s-2} = P_{s-1} \quad \text{and} \quad Q_{s-1}\, D_0 = a_0(Q_{s-1}\, a_0 + Q_{s-2}) + P_{s-1}\, a_0 + P_{s-2},$$

whence

$$D_0 = a_0^2 + \frac{a_0(Q_{s-2} + P_{s-1}) + P_{s-2}}{Q_{s-1}}.$$

Let

$$a = a_0 + Q_{s-1}\, k, \qquad \text{where} \qquad k = 1, 2, 3, \ldots$$

Then the number

$$\frac{a\,(Q_{s-2} + P_{s-1}) + P_{s-2}}{Q_{s-1}} = \frac{a_0(Q_{s-2} + P_{s-1}) + P_{s-2}}{Q_{s-1}} + (Q_{s-2} + P_{s-1})\, k$$
$$= D_0 - a_0^2 + (Q_{s-2} + P_{s-1})\, k$$

is natural and $\leqslant 2a + 1$, since

$$\frac{Q_{s-2} + P_{s-1}}{Q_{s-1}} < \frac{2Q_{s-1}}{Q_{s-1}} = 2 \qquad \text{and} \qquad \frac{P_{s-2}}{Q_{s-1}} < 1.$$

Therefore the number

$$D = a^2 + \frac{a(Q_{s-2}+P_{s-1})+P_{s-2}}{Q_{s-1}}$$

is natural and $[\sqrt{D}] = a$. Moreover, since $Q_{s-2} = P_{s-1}$,

$$\sqrt{D} = a + \frac{P_{s-1}(a+\sqrt{D})+P_{s-2}}{Q_{s-1}(a+\sqrt{D})+Q_{s-2}},$$

we have

$$\sqrt{D} = a + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1\ |}{|a_{s-1}} + \frac{1\ |}{|a+\sqrt{D}}.$$

Then the number

$$\begin{aligned} D &= (a_0 + Q_{s-1}k)^2 + D_0 - a_0^2 + (Q_{s-2}+P_{s-1})k \\ &= Q_{s-1}^2 k^2 + (2a_0 Q_{s-1} + Q_{s-2} + P_{s-1})k + D_0, \end{aligned}$$

where $k = 1, 2, \ldots$, satisfies the condition of the theorem, the proof of which is thus completed. □

We now prove the following

THEOREM 6. *For any natural number s there exist infinitely many natural numbers D such that the representation of the number $\sqrt{D}$ as a simple continued fraction has a period consisting of s terms.*

LEMMA. *If n is a natural number > 1 and $a_1, a_2, \ldots, a_n$ a symmetric sequence of natural numbers, and if, moreover, P_k/Q_k denotes the k-th convergent of the continued fraction*

$$\frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_n},$$

then

$$P_n = Q_{n-1}.$$

PROOF OF THE LEMMA. In view of formulae (3) we have

$$Q_n = Q_{n-1}a_n + Q_{n-2},\ Q_{n-1} = Q_{n-2}a_{n-1} + Q_{n-3}, \ldots, Q_2 = a_2 a_1 + 1,$$
$$Q_1 = a_1.$$

Hence

$$\frac{Q_n}{Q_{n-1}} = a_n + \frac{1\ |}{|a_{n-1}} + \frac{1\ |}{|a_{n-2}} + \ldots + \frac{1|}{|a_2} + \frac{1|}{|a_1}.$$

But, since the sequence $a_1, a_2, \ldots, a_n$ is symmetric, this gives

$$\frac{Q_n}{Q_{n-1}} = a_1 + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_n} \quad \text{and so} \quad \frac{Q_{n-1}}{Q_n} = \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_n}$$
$$= \frac{P_n}{Q_n},$$

whence $P_n = Q_{n-1}$, which was to be proved. ☐

REMARK. If by Q_0 we understand number 1, then the lemma is true for $n = 1$ as well.

PROOF OF THEOREM 6. Let k and n be two given natural numbers and let $a_1, a_2, \ldots, a_n$ be a sequence whose terms are all equal to $2k$. In virtue of the lemma, $P_n = Q_{n-1}$. For an integer $t \geqslant 0$ we denote by y_t the number

$$y_t = (Q_n t + k; \overline{2k, 2k, \ldots, 2k, 2Q_n t + 2k}),$$

where the sequence $2k, 2k, \ldots, 2k$ has n terms. Then

$$y_t = Q_n t + k + \frac{1|}{|2k} + \frac{1|}{|2k} + \ldots + \frac{1|}{|2k} + \frac{1\qquad|}{|Q_n t + k + y}.$$

Hence, since $Q_{n-1} = P_n$, we have

$$y_t - Q_n t - k = \frac{P_n(Q_n t + k + y_t) + P_{n-1}}{Q_n(Q_n t + k + y_t) + P_n}.$$

So

$$Q_n(y_t^2 - (Q_n t + k)^2) = 2P_n(Q_n t + k) + P_{n-1}.$$

Thus, in particular, for $t = 0$ we obtain

$$Q_n(y_0^2 - k^2) = 2P_n k + P_{n-1}.$$

On the other hand, by the definition of the numbers y_t, $y_0 = (k; \overline{2k}) = \sqrt{k^2+1}$. Consequently, $Q_n = 2P_n k + P_{n-1}$ and so $y_t^2 = (Q_n t + k)^2 + 2P_n t + 1$, whence $y_t = \sqrt{(Q_n t + k)^2 + 2P_n t + 1}$. Hence it follows that for natural numbers k and integers $t \geqslant 0$ the simple continued fraction for the square root of the number $D = (Q_n t + k)^2 + 2P_n t + 1$ has a period consisting of $n+1$ terms, each of the first n terms being equal to $2k$. Taking into account the fact that the period $(k; \overline{2k}) = \sqrt{k^2+1}$ has one term only, we see that the proof of Theorem 6 is completed. ☐

For example, for $k = 1$ and $n = 1, 2, 3, 4, 5, 6$ we find for $t = 0, 1, 2, \ldots$, respectively (cf. Kraïtchik [1], p. 57)

$$\begin{aligned}
\sqrt{(2t+1)^2+2t+1} &= (2t+1;\overline{2, 4t+2}),\\
\sqrt{(5t+1)^2+4t+1} &= (5t+1;\overline{2, 2, 10t+2}),\\
\sqrt{(12t+1)^2+10t+1} &= (12t+1;\overline{2, 2, 2, 24t+2}),\\
\sqrt{(29t+1)^2+24t+1} &= (29t+1;\overline{2, 2, 2, 2, 58t+2}),\\
\sqrt{(70t+1)^2+58t+1} &= (70t+1;\overline{2, 2, 2, 2, 2, 140t+2}),\\
\sqrt{(169t+1)^2+140t+1} &= (169t+1;\overline{2, 2, 2, 2, 2, 2, 338t+2}).
\end{aligned}$$

Hence, in particular, for $t = 1$, we obtain

$$\sqrt{12} = (3;\overline{2, 6}), \qquad \sqrt{41} = (6;\overline{2, 2, 12}),$$

$$\sqrt{180} = (13;\overline{2, 2, 2, 26}), \qquad \sqrt{925} = (30;\overline{2, 2, 2, 2, 60}).$$

It can be proved that for every number n of the form $3k$ or $3k+1$ there exist infinitely many natural numbers D such that the representation of the number $\sqrt{D}$ as a simple continued fraction has a period consisting of $n+1$ terms, each of the first n terms being equal to 1 (cf. Sierpiński [26], p. 300).

For example we have for $t = 1, 2, \ldots$

$$\sqrt{(89t-44)^2+110t-54} = (89t-44;\overline{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 178t-88}).$$

Hence, for $t = 1$,

$$\sqrt{2081} = (45;\overline{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 90}).$$

W. Patz [1] has tabulated the representations of the irrational numbers $\sqrt{D}$, with $D < 10000$, as simple continued fractions.

It follows from the tables that among the first hundred natural numbers the longest period is that of the number

$$\sqrt{94} = (9;\overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}),$$

which consists of 16 terms.

The number $\sqrt{919}$ has a period consisting of 60 terms:

$$\begin{aligned}
\sqrt{919} = (30;\ &\overline{3, 5, 1, 2, 1, 2, 1, 1, 1, 2, 3, 1, 19, 2, 3, 1, 1, 4, 9, 1,}\\
&\overline{7, 1, 3, 6, 2, 11, 1, 1, 1, 29, 1, 1, 1, 11, 2, 6, 3, 1, 7, 1,}\\
&\overline{9, 4, 1, 1, 3, 2, 19, 1, 3, 2, 1, 1, 1, 2, 1, 2, 1, 5, 3, 60})
\end{aligned}$$

(Kraïtchik [1], p. 57 gives by mistake the number of terms as 62).

The number $\sqrt{991}$ has a period consisting of 60 terms:

$$\sqrt{991} = (31;\overline{2, 12, 10, 2, 2, 2, 1, 1, 2, 6, 1, 1, 1, 1, 3, 1, 8, 4, 1, 2, 1,}$$
$$\overline{2, 3, 1, 4, 1, 20, 6, 4, 31, 4, 6, 20, 1, 4, 1, 3, 2, 1, 2,}$$
$$\overline{1, 4, 8, 1, 3, 1, 1, 1, 1, 6, 1, 1, 2, 2, 2, 10, 12, 2, 62}).$$

It will be observed that

$$\sqrt{1000} = (31;\overline{1, 1, 1, 1, 1, 6, 2, 2, 15, 2, 2, 15, 2, 2, 6, 1, 1, 1, 1, 1, 62}).$$

Any irrational root of a polynomial of the second degree with integral coefficients is called *quadratic irrational.*

If x is a real irrational number satisfying the equation $Ax^2+Bx+C = 0$, where A, B, C are integers, then, as is known, $D = B^2-4AC > 0$ and D is not the square of a natural number. We have $x = (-B\pm\sqrt{D})/2A$.

The following theorem of Lagrange is proved by suitable changes in the proof of Theorem 3.

The representation of a real quadratic irrational as a simple continued fraction is periodic. Conversely, every periodic simple continued fraction represents a real quadratic irrational (Lagrange, see Kraïtchik [1], pp. 9-13).

EXAMPLE. We have $\frac{1}{2}(\sqrt{5}+1) = (1;\overline{1})$. This follows immediately from the equality $\frac{1}{2}(\sqrt{5}+1) = 1+1/(\frac{1}{2}(\sqrt{5}+1))$.

EXERCISES. **1.** Prove that any real number is a sum of two numbers, each of them representable by a simple continued fraction with the first quotient equal to 1.

PROOF. As we have learned in § 3, in order that the first quotient of the simple continued fraction for a real number t equals to 1 it is necessary and sufficient that $t-[t] \geqslant \frac{1}{2}$(1). For a real number x we set $u = \frac{1}{2}(x-[x])+\frac{1}{2}$, $v = [x]-1+u$. Then, clearly, $x = u+v$ and, since $0 \leqslant x-[x] < 1$, we have $\frac{1}{2} \leqslant u < 1$, whence $[v] = [x]-1$, and so $v-[v] = u \geqslant \frac{1}{2}$. These inequalities give the desired result by the above remark. □

REMARK. M. Hall, Jr., [1] has proved that each real number is a sum of two numbers, each of them representable by a simple continued fraction with no quotient greater than 4.

Even if a number x is known within the accuracy of $1/10^{100}$ we are in general unable to find the first quotient of its representation as a simple continued fraction. In fact, if the only thing we know is that $0 < x < 1/10^{100}$, then we may conclude that $1/x > 10^{100}$, i.e. that the first quotient of the representation of x as a simple continued fraction is $\geqslant 10^{100}$.

---

(1) This is true because $t-[t] = \frac{1}{2}$ gives $t = [t]+\frac{1|}{|1}+\frac{1|}{|1}$.

2. Prove that there is no natural number D such that $\sqrt{D}$ could be represented as a simple continued fraction with a period consisting of 6 terms, the first five being equal to 1.

PROOF. Suppose that such a D exists. Then

$$\sqrt{D} = a_0 + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1\ \ |}{|a_0+\sqrt{D}}.$$

Denote by P_n/Q_n the nth convergent of the simple continued fraction $\frac{1|}{|1} + \frac{1|}{|1} + \dots$

We have

$$\sqrt{D} - a_0 = \frac{P_5(a_0+\sqrt{D})+P_4}{Q_5(a_0+\sqrt{D})+Q_4} = \frac{5(a_0+\sqrt{D})+3}{8(a_0+\sqrt{D})+5},$$

whence

$$D = a_0^2 + \frac{10a_0+3}{8},$$

which is impossible because the odd number $10a_0+3$ is not divisible by 8. ☐

3. Let $f(s)$ denote the least natural number D such that the period of the simple continued fraction of $\sqrt{D}$ consists of s terms. Find the values of $f(s)$ for $s \leqslant 10$.

ANSWER. $f(1) = 2$, $\sqrt{2} = (1; 2)$; $f(2) = 3$, $\sqrt{3} = (1; \overline{1,2})$; $f(3) = 41$, $\sqrt{41} = (6; \overline{2, 2, 12})$; $f(4) = 7$, $\sqrt{7} = (2; \overline{1, 1, 1, 4})$; $f(5) = 13$, $\sqrt{13} = (3; \overline{1, 1, 1, 1, 6})$; $f(6) = 19$, $\sqrt{19} = (4; \overline{2, 1, 3, 1, 2, 8})$; $f(7) = 58$, $\sqrt{58} = (7; \overline{1, 1, 1, 1, 1, 1, 14})$; $f(8) = 31$, $\sqrt{31} = (5; \overline{1, 1, 3, 5, 3, 1, 1, 10})$; $f(9) = 106$, $\sqrt{106} = (10; \overline{3, 2, 1, 1, 1, 1, 2, 3, 20})$; $f(10) = 43$, $\sqrt{43} = (6; \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12})$.

5. Application of the continued fraction for $\sqrt{D}$ in solving the equations $x^2 - Dy^2 = 1$ and $x^2 - Dy^2 = -1$.

Let D be a natural number which is not the square of a natural number. Let $\sqrt{D} = (a_0; \overline{a_1, a_2, \dots, a_s})$ be the simple continued fraction for $\sqrt{D}$, and P_k/Q_k the kth convergent to it. We have

$$\sqrt{D} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a} + \dots + \frac{1\ |}{|a_{s-1}} + \frac{1\ \ \ |}{|a_s - a_0 + \sqrt{D}}.$$

Hence

$$\sqrt{D} = P_{s-1}(a_s - a_0 + \sqrt{D}) + P_{s-2}Q_{s-1}(a_s - a_0 + \sqrt{D}) + Q_{s-2}$$

and, more generally, since $a_0 = a_s - a_0$,

$$\sqrt{D} = \frac{P_{ks-1}(\sqrt{D}+a_0)+a_0)+P_{ks-2}}{Q_{ks-1}(\sqrt{D}+a_0)+Q_{ks-2}} \quad \text{for} \quad k = 1, 2, 3, \dots,$$

whence, in view of the fact that $\sqrt{D}$ is irrational,

$$a_0 Q_{ks-1} - P_{ks-1} = -Q_{ks-2} \quad \text{and} \quad DQ_{ks-1} - a_0 P_{ks-1} = P_{ks-2}.$$

Multiplying the first equality by $-P_{ks-1}$ and the second by $-Q_{ks-1}$ and then adding them, we obtain by (6),

$$P_{ks-1}^2 - DQ_{ks-1}^2 = Q_{ks-2} - P_{ks-1} - P_{ks-2}\, Q_{ks-1} = (-1)^{ks}.$$

If s is **odd**, then this equality gives

$$(43) \qquad P_{ks-1}^2 - DQ_{ks-1}^2 = \begin{cases} -1 & \text{for} \quad k = 1, 3, 5, \ldots \\ 1 & \text{for} \quad k = 2, 4, 6, \ldots \end{cases}$$

If s is even, then

$$(44) \qquad P_{ks-1}^2 - DQ_{ks-1}^2 = 1 \quad \text{for any} \quad k = 1, 2, 3, \ldots$$

Thus we see that some of the convergents of the simple continued fraction for $\sqrt{D}$ are solutions of the equation $x^2 - Dy^2 = 1$ in natural numbers. We show that the converse is also true: any solution of the equation in natural numbers gives the numerator and the denominator of a convergent of the simple continued fraction for $\sqrt{D}$.

Accordingly we assume that t and u are a solution of the equation $x^2 - Dy^2 = 1$ in natural numbers. We have $t > u$.

Let

$$(45) \qquad \frac{t}{u} = \frac{1|}{|b_1} + \frac{1|}{|b_2} + \ldots + \frac{1\ |}{|b_{k-1}}$$

be the representation of number t/u as a simple continued fraction, k being even. To see that such a representation exists we note that, if $k-1$ were even, then for $b_{k-1} > 1$ the number $b_{k-1} - 1 + \frac{1|}{|1}$ could be written in place of b_{k-1}, and for $b_{k-1} = 1$ the number $b_{k-2} + 1$ could be written in place of $b_{k-2} + \frac{1\ |}{|b_{k-1}}$.

Let t'/u' be the last but one convergent of the simple continued fraction (45). Then

$$(45^a) \qquad \frac{t'}{u'} = b_0 + \frac{1|}{|b_1} + \frac{1|}{|b_2} + \ldots + \frac{1\ |}{|b_{k-2}}.$$

We have $u' < u$. (For $k = 2$ we have $t'/u' = b_0$.) Since k is even, by (6) we have $tu'-ut' = 1$. Now, subtracting the last equality from the equality $t^2-Du^2 = 1$, we obtain

$$t(u'-t) = u(t'-Du). \tag{46}$$

In virtue of (45) we have $0 < t/u-b_0 \leqslant 1$, whence

$$0 < t-b_0 u \leqslant u. \tag{47}$$

In view of the fact that t and u are relatively prime (because $t^2-Du^2 = 1$), we see that for an integer l the equalities

$$u'-t = lu, \qquad t'-Du = lt \tag{48}$$

hold. Hence

$$u'-(t-b_0 u) = (l+b_0)u. \tag{49}$$

From the inequalities $0 < u' < u$ and (47) we infer that $|u'-(t-b_0 u)| < u$, which in virtue of (49) gives $l+b_0 = 0$, so $l = -b_0$, whence, by (48)

$$u' = t-b_0 u, \qquad t' = Du-b_0 t,$$

and consequently

$$\frac{t(b_0+\sqrt{D})+t'}{u(b_0+\sqrt{D})+u'} = \frac{t\sqrt{D}+Du}{t+u\sqrt{D}} = \sqrt{D}; \tag{50}$$

but, by (45) and (45^a), the left-hand side of (50) is equal to

$$b_0+\frac{1|}{b_1}+\frac{1|}{|b_2}+\ldots+\frac{1|}{|b_{k-1}}+\frac{1|}{|b_0+\sqrt{D}};$$

so, by (50), the simple continued fraction for $\sqrt{D}$ is $\sqrt{D} = (b_0; b_1, b_2, \ldots, b_{k-1}, 2b_0)$, the $(k-1)$-th convergent of which being number (45). It follows from what we stated above that number k is equal to the number of the terms of the period of the simple continued fraction for $\sqrt{D}$. This period need not be the shortest one. Denote by s the shortest period of this continued fraction. Clearly, $s \mid k$ and so $k = sn$, where n is a natural number. For any solution of the equation $x^2-Dy^2 = 1$ in natural numbers t and u, number t/u is a convergent of the simple continued fraction for $\sqrt{D}$; namely it is the $(ns-1)$-th convergent, where s is the number of terms of the shortest period of the continued fraction and n a natural number. According to what we have proved above (cf. formula (44)), if s is an even number, then any $(ns-1)$-th convergent ($n = 1, 2, \ldots$) defines a solution of the equation $x^2-Dy^2 = 1$ in natural numbers. Thus we have proved the following

THEOREM 7. *If the period of the simple continued fraction for number* $\sqrt{D}$ *consists of an even number* s *of terms, then the numerator and the denominator of the* $(ns-1)$*-th convergent,* $n = 1, 2, \ldots,$ *form a solution of the equation* $x^2 - Dy^2 = 1$ *in natural numbers. Moreover, all the solutions are obtained in this way.*

From this we see that the solution in the least natural numbers is given by the $(s-1)$-th convergent.

If s is odd, then formulae (43) show that the numerator and the denominator of the $(ns-1)$-th convergent form a solution of the equation $x^2 - Dy^2 = 1$ only in the case where n is an even number. Hence

THEOREM 8. *If the period of the simple continued fraction for* $\sqrt{D}$ *consists of an odd number* s *of terms, then the numerator and the denominator of the* $(2ns-1)$*-th convergent,* $n = 1, 2, \ldots$ *form the solution of the equation* $x^2 - Dy^2 = 1$ *in natural numbers. Moreover, all the solutions are obtained in this way.*

Thus we see that in this case the solution in the least natural numbers is given by the $(2s-1)$-th convergent.

The representation of number $\sqrt{991}$ as a simple continued fraction was given above. We saw that its period consists of 60 terms. This representation and Theorem 7 were the basis for calculating the least solution of the equation $x^2 - 991y^2 = 1$ in natural numbers, which was given in Chapter II, § 15. In this solution number x has 30 digits, number y 29 digits.

Now we turn to the equation

$$x^2 - Dy^2 = -1. \tag{51}$$

Suppose that $D = a^2+1$, where a is a natural number > 1. As we have already learned, we have $\sqrt{a^2+1} = (a; \overline{2a})$. Hence, if P_k/Q_k is the kth convergent of $(a; \overline{2a})$, then by (43), since $s = 1$, we obtain

$$P_{k-1}^2 - DQ_{k-1}^2 = -1, \qquad k = 1, 3, 5, \ldots$$

Thus the solution in the least natural numbers of the equation are the numbers $t = P_0 = a$, $u = Q_0 = 1$. For the other solutions of (51) in natural numbers, t, u we have $u > 1$. If $D \neq a^2+1$, a being a natural number, then, if t and u are a solution of equation (51) in natural numbers, we also have $u > 1$ because, if u were equal to 1, we would have

$t^2 - D = -1$, whence $D = t^2 + 1$, contrary to the assumption concerning number D. Therefore in what follows we may assume that t and u are a solution of (51) in natural numbers with $u > 1$. Again let (45) be the simple continued fraction for the number t/u, this time k being an odd number. We define also the number t'/u' by (45^a). Since now k is odd, we have $tu' - ut' = -1$, whence, in view of the formula $t^2 - Du^2 = -1$, we again obtain (46).

An argument similar to that used in the previous case shows that number (45) is the $(k-1)$-th convergent of the simple continued fraction for number $\sqrt{D}$ and that $k = sn$, where s is the number of the terms of the (least) period of the continued fraction for $\sqrt{D}$ and n is a natural number. But, if s is even, then, by (44), none of the $(sn-1)$-th convergents gives a solution of equation (51). If, conversely, s is odd, then, by (43) the $sn-1$ convergents give solutions of (51), provided n is odd. Thus we arrive at

THEOREM 9. *If the period of the simple continued fraction for number* $\sqrt{D}$ *has* s *terms and if* s *is even, then equation* (51) *has no solutions in natural numbers. If* s *is odd, then the numerator and the denominator of each of the* $((2n-1)s-1)$*-th convergents,* $n = 1, 2, \ldots$, *form a solution of equation* (51) *in natural numbers. Moreover, all the solutions are obtained in this way.*

EXAMPLES. **1.** Let $D = 2$. Since $D = (1; \overline{2})$, we have $s = 1$ and so, by Theorem 7, we infer that the numerator and the denominator of any of the $(2n-1)$-th convergents, $n = 1, 2, \ldots$ form a solution of the equation $x^2 - 2y^2 = 1$ in natural numbers, and, moreover, all the solutions are obtained in this way. The first convergent, i.e. the number $1 + \frac{1}{2} = \frac{3}{2}$, gives the solution in the least natural numbers, $x = 3$, $y = 2$. In virtue of Theorem 9 the numerator and the denumerator of any of the $(2n-2)$-th convergents, $n = 1, 2, \ldots$, form a solution of the equation $x^2 - 2y^2 = -1$ in natural numbers, and all the solutions are obtained in this way. The 0-th convergent, i.e. number $1/1$ gives the solution of the equation in the least natural numbers.

2. Let $D = 3$. Then $\sqrt{3} = (1; \overline{1, 2})$. We have $s = 2$, and so, by Theorem 7, the numerator and the denominator of the $(2n-1)$-th convergents, $n = 1, 2, \ldots$, form a solution of the equation $x^2 - 3y^2 = 1$ and all the solutions are obtained in this way. The solution in the least natural numbers is given by the first convergent, i.e. by number $1 + \frac{1}{1} = \frac{3}{2}$, whence, $x = 3$, $y = 2$. However, in view of Theorem 9, the equation $x^2 - 3y^2 = -1$ has no solutions in natural numbers.

3. Let $D = 13$. Then $\sqrt{13} = (3; \overline{1, 1, 1, 1, 6})$. We have $s = 5$, and so, by Theorem 8, the numerator and the denominator of any of the $(10n-1)$-th convergents, $n = 1, 2, \ldots$, gives the solution of the equation $x^2-13y^2 = 1$, and all the solutions are obtained in this way. The solution in the least natural numbers is given by the 9-th convergent, i.e. by the number

$$3+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|6}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}=\frac{649}{180},$$

whence $x = 649$, $y = 180$.

In view of Theorem 9 the numerator and the denominator of any of the $(10n-6)$-th convergents, $n = 1, 2, \ldots$, is a solution of the equation $x^2-13y^2 = -1$ and all the solutions are obtained in this way. The solution in the least natural numbers is given by the 4-th convergent, i.e. by the number

$$3+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}+\frac{1|}{|1}=\frac{18}{5},$$

whence $x = 18$, $y = 5$.

It is really not at difficult to find the solutions of the equation $x^2-Dy^2 = -1$ in the least natural numbers by the use of the representation of number $\sqrt{D}$ as a simple continued fraction for $D < 100$. The table of such solutions for $D \leqslant 1003$ has been given already by Legendre [1].

Here are the solutions in the least natural numbers of the equation $x^2-Dy^2 = 1$ for $D \leqslant 40$.

D	x	y	D	x	y	D	x	y
2	3	2	15	4	1	28	127	24
3	2	1	17	33	8	29	4901	1820
5	9	4	18	17	4	30	11	2
6	5	2	19	170	39	31	1520	273
7	8	3	20	9	2	32	17	3
8	3	1	21	55	12	33	23	4
10	19	6	22	197	42	34	35	6
11	10	3	23	24	5	35	6	1
12	7	2	24	5	1	37	73	12
13	649	180	26	51	10	38	37	6
14	15	4	27	26	5	39	25	4
						40	19	3

From Theorem 8 it follows that the equation $x^2-Dy^2 = -1$ is solvable in natural numbers for $D \leqslant 100$ only in the case where D is one of the numbers

2, 5, 10, 13, 17, 26, 29, 37, 41, 50, 53, 58, 61, 65, 73, 74, 82, 85, 89, 97.

6. Continued fractions other than simple continued fractions

Fractions of the form

$$a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \ldots + \frac{b_n|}{|a_n}, \tag{52}$$

where $a_0, a_1, \ldots, a_n, b_1, b_2, \ldots, b_n$ are arbitrary real or complex numbers have been investigated.

A numerical value can be assigned to symbol (52) if and only if all

$$a_n \neq 0,\ a_{n-1} + \frac{b_n}{a_n} \neq 0,\ a_{n-2} + \frac{b_{n-2}|}{|a_{n-1}} + \frac{b_n|}{|a_n} \neq 0,\ \ldots$$

$$\ldots,\ a_1 + \frac{b_2|}{|a_2} + \ldots + \frac{b_n|}{|a_n} \neq 0.$$

We see that some (or even all) of the numbers $a_1, a_2, \ldots, a_{n-1}$ may be equal to zero; for example as is easily shown, the continued fraction $\frac{1|}{|0} + \frac{1|}{|0} + \ldots + \frac{1|}{|0} + \frac{1|}{|2}$ is equal to 2.

It can be proved that *if a continued fraction*

$$R_n = a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \ldots + \frac{b_n|}{|a_n} \tag{53}$$

has a well-defined value and if the numbers P_k *and* Q_k $(k = 0, 1, \ldots, n)$ *are given by the inductive formulae*

$$P_0 = a_0,\ Q_0 = 1,\ P_1 = a_0 a_1 + b_1,\ Q_1 = a_1,$$

$$P_k = P_{k-1} a_k + P_{k-2} b_k,\ Q_k = Q_{k-1} a_k + Q_{k-2} b_k,\ k = 2, 3, \ldots, n,$$

then

$$R_n = \frac{P_n}{Q_n} \text{ and } P_{k-1} Q_k - Q_{k-1} P_k = (-1)^k b_1 b_2 \ldots b_k \text{ for } k = 1, 2, \ldots, n.$$

We note that even if the continued fraction (52) has a well-defined value, it may happen that some of its convergents do not have this property. For example, the fraction $\frac{1|}{|1} + \frac{-1|}{|\ 1} + \frac{1|}{|1}$ has the value 2, but the convergent $\frac{1|}{|1} + \frac{-1|}{|\ 1}$ has no value.

If the sequences $a_0, a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ are infinite and if the sequence of numbers (53) is convergent to a limit x, then x is called the *value* of the infinite continued fraction:

$$x = a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \ldots \tag{54}$$

Examples of such infinite continued fractions are provided by the formula of Brouncker for number $\pi/4$, found in the year 1655,

$$\frac{\pi}{4} = \frac{1|}{|1} + \frac{1^2|}{|2} + \frac{3^2|}{|2} + \frac{5^2|}{|2} + \ldots$$

and the formula for log 2,

$$\log 2 = \frac{1|}{|1} + \frac{1^2|}{|1} + \frac{2^2|}{|1} + \frac{3^2|}{|1} + \ldots$$

The former easily follows from the identity

$$\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \ldots + \frac{(-1)^{n-1}}{2n-1} = \frac{1|}{|1} + \frac{1^2|}{|2} + \frac{3^2|}{|2} + \frac{5^2|}{|2} + \ldots + \frac{(2n-3)^2|}{|2}$$

and from the well-known formula of Leibniz for $\pi/4$; the latter follows from the identity

$$\frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \ldots + \frac{(-1)^{n-1}}{n} = \frac{1|}{|1} + \frac{1^2|}{|1} + \frac{2^2|}{|1} + \frac{3^2|}{|1} + \ldots + \frac{(n-1)^2|}{|1}$$

for natural numbers n (¹).

We now turn to some special cases of continued fractions like (54).

For a real number x_0 we denote by $G(x_0)$ the least integer $> x_0$. We then have $x_0 < G(x_0) \leqslant x_0+1$, whence $0 < G(x_0)-x_0 \leqslant 1$ and consequently $x_1 = \dfrac{1}{G(x_0)-x_0} \geqslant 1$. Hence $G(x_1) \geqslant 2$. We repeat this procedure with x_1 in place of x_0 and so on. Thus, if $x_n = \dfrac{1}{G(x_{n-1})-x_{n-1}}$ for $n = 1, 2, \ldots$, we have $x_n \geqslant 1$ and $G(x_n) \geqslant 2$, $n = 1, 2, \ldots$ Moreover,

$$x_0 = G(x_0) + \frac{-1\ |}{|\,G(x_1)} + \frac{-1\ |}{|\,G(x_2)} + \ldots + \frac{-1\ |}{|\,G(x_{n-1})} + \frac{-1|}{|\,x_n}.$$

(¹) The proofs of the formulae are to be found in Sierpiński [7], Part II, p. 140.

It can be proved that this leads to an infinite continued fraction for the number x_0:

$$x_0 = G(x_0)+\frac{-1\,|}{|\,G(x_1)}+\frac{-1\,|}{|\,G(x_2)}+\frac{-1\,|}{|\,G(x_2)}+\ldots \tag{55}$$

Thus we see that any real number x is representable as an infinite continued fraction of the form

$$x = a_0-\frac{1\,|}{|\,a_1}-\frac{1\,|}{|\,a_2}-\frac{1\,|}{|\,a_3}-\ldots,$$

where a_0 is an integer and a_n are natural numbers $\geqslant 2$. It can be proved that every real number has precisely one such representation. In particular, we have

$$1 = 2-\frac{1|}{|2}-\frac{1|}{|2}-\frac{1|}{|2}-\ldots$$

It is a property of rational numbers that in their representations in form (55) we have $G(x_n) = 2$ for sufficiently large n.

The formula

$$\sqrt{2} = 2-\frac{1|}{|2}-\frac{1\,|}{|\,2+\sqrt{2}}$$

gives the representation of $\sqrt{2}$ as a continued fraction with a period consisting of two terms,

$$\sqrt{2} = 2-\frac{1|}{|2}-\frac{1|}{|4}-\frac{1|}{|2}-\frac{1|}{4}-\ldots$$

Another type of representation of a real number x by a continued fraction is the one in which a_0 is the nearest integer to x and x_1 is the number given by the formula $x = a_0 \pm 1/x_1$ where the sign $+$ or $-$ is taken depending on whether $x > a_0$ or $x < a_0$. By the use of x_1 we define a_1 and x_2 in the same way as a_0 and x_1 was defined by x, and so on (cf. Hurwitz [1]).

A representation of this type of $\sqrt{2}$ is the same as the simple continued fraction for $\sqrt{2}$. For $\sqrt{3}$, however, we have

$$\sqrt{3} = 2-\frac{1|}{|4}-\frac{1|}{|4}-\ldots$$

i.e. a representation of form (55). For $\sqrt{5}$ the representation coincides with the simple continued fraction for $\sqrt{5}$, and for $\sqrt{7}$ we have

$$\sqrt{7} = 3 - \frac{1|}{|3} - \frac{1|}{|6} - \frac{1|}{|3} - \dots,$$

i.e. a representation of type (55) again. But for $\sqrt{13}$ we have

$$\sqrt{13} = 4 - \frac{1|}{|3} - \frac{1|}{|2} + \frac{1\quad|}{|3+\sqrt{13}},$$

which gives the representation

$$\sqrt{13} = 4 - \frac{1|}{|3} - \frac{1|}{|2} + \frac{1|}{|7} - \frac{1|}{|3} - \frac{1|}{|2} + \frac{1|}{|7} - \dots,$$

which is neither of type (55) nor a simple continued fraction.

To close this chapter we consider the following continued fraction

$$a_0 + \cfrac{a_1 + \cfrac{a_2 + \dots}{b_2}}{b_1} = a_0 + \frac{|a_1}{b_1|} + \frac{|a_2}{b_2|} + \dots = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_1 b_2} + \frac{a_3}{b_1 b_2 b_3} + \dots$$

Let $b_1, b_2, \dots$ be an infinite sequence of natural numbers among which there are infinitely many numbers different from 1. Let x_0 denote a real number and let $a_0 = [x_0]$, $a_1 = [b_1(x_0 - a_0)]$. Clearly, a_1 is an integer $< b_1$. Let $x_1 = b_1(x_0 - a_0) - a_1$. We then have $0 \leqslant x_1 < 1$. In general, suppose that for a natural number $n > 1$ we are given the number x_{n-1}; then we put $a_n = [b_n x_{n-1}]$ and $x_n = b_n x_{n-1} - a_n$. Thus the sequence $a_1, a_2, \dots$ is defined by induction and its terms are non-negative integers such that $a_n < b_n$, as well as the sequence $x_1, x_2, \dots$ of real numbers with $0 \leqslant x_n < 1$, for any $n = 1, 2, \dots$ Hence, we easily obtain

$$(56) \qquad x_0 = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_1 b_2} + \dots + \frac{a_n}{b_1 b_2 \dots b_n} + \frac{x_n}{b_1 b_2 \dots b_n}.$$

By assumption, numbers $b_1, b_2, \dots$ are natural and infinitely many of them are $\geqslant 2$. Therefore the product $b_1 b_2 \dots b_n$ increases to infinity with n. Moreover, since $0 \leqslant x_n < 1$, formula (56) gives a representation of x_0 as the infinite series

$$(57) \qquad x_0 = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_1 b_2} + \frac{a_3}{b_1 b_2 b_3} + \dots,$$

i.e. as the infinite continued fraction

$$x_0 = a_0 + \frac{|a_1}{b_1|} + \frac{|a_2}{b_2|} + \ldots \tag{58}$$

This proves the following theorem:

For any infinite sequence of natural numbers $b_1, b_2, \ldots$ *in which infinitely many terms are different from* 1, *any real number* x_0 *may be represented as an infinite continued fraction of form* (58), *where* $a_0 = [x_0]$, a_n $(n = 1, 2, \ldots)$ *are integers* $0 \leqslant a_n < b_n$ *for* $n = 1, 2, \ldots$

As is easy to see, representation (57) coincides with the representation as a decimal with the varying base which was considered in Chapter VII, § 6.

CHAPTER IX

LEGENDRE'S SYMBOL AND JACOBI'S SYMBOL

1. Legendre's symbol $\left(\dfrac{D}{p}\right)$ and its properties

If p is an odd prime and D an integer not divisible by p, Legendre's symbol $\left(\dfrac{D}{p}\right)$ is said to be equal to 1 if D is a quadratic residue to the modulus p, and it is said to be equal to -1 if D is a quadratic non-residue to p.

In view of theorem 4 of Chapter V, we have

$$(1)\qquad \left(\frac{D}{p}\right) \equiv D^{\frac{1}{2}(p-1)} (\operatorname{mod} p).$$

Consequently, the value of $\left(\dfrac{D}{p}\right)$ is 1 if and only if $D^{(p-1)/2}$ divided by p leaves the remainder 1.

By Theorem 15 of Chapter VI, we have

$$(2)\qquad \left(\frac{D}{p}\right) = (-1)^{\operatorname{ind} D},$$

where the indices are taken relative to a primitive root of the prime p.

If D and D' are integers not divisible by a prime p, then, by (1), the following property holds:

I. *If* $D \equiv D' (\operatorname{mod} p)$, *then* $\left(\dfrac{D}{p}\right) = \left(\dfrac{D'}{p}\right)$.

From (2) it follows that if D and D' are integers not divisible by p, then

$$(3)\qquad \left(\frac{DD'}{p}\right) = (-1)^{\operatorname{ind} DD'} \quad \text{and} \quad \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = (-1)^{\operatorname{ind} D + \operatorname{ind} D'}.$$

But, according to property II of indices (see Chapter VI, § 8), we have $\operatorname{ind} DD' \equiv \operatorname{ind} D + \operatorname{ind} D' (\operatorname{mod} p-1)$. Hence, since p is an odd prime, and *a fortiori*, we have $\operatorname{ind} DD' \equiv \operatorname{ind} D + \operatorname{ind} D' (\operatorname{mod} 2)$, whence $(-1)^{\operatorname{ind} DD'} = (-1)^{\operatorname{ind} D + \operatorname{ind} D'}$. Consequently, by (3), $\left(\dfrac{DD'}{p}\right) = \left(\dfrac{D}{p}\right)\left(\dfrac{D'}{p}\right)$. Thus we have proved

II. *If D and D′ are integers not divisible by p, then*

$$\left(\frac{DD'}{p}\right)=\left(\frac{D}{p}\right)\left(\frac{D'}{p}\right).$$

Now we prove (cf. Sierpiński [2]) that if $\left\{\frac{D}{p}\right\}$ is a real number defined for a fixed odd prime p and any integer D not divisible by p, which is different from zero for at least one value of D and different from 1 for at least one D and which, moreover, satisfies the conditions

1° if $D\equiv D' \pmod{p}$, then $\left\{\frac{D}{p}\right\}=\left\{\frac{D'}{p}\right\}$,

2° $\left\{\frac{DD'}{p}\right\}=\left\{\frac{D}{p}\right\}\left\{\frac{D'}{p}\right\}$ for any D and D' that are not divisible by p,

then for any integer D not divisible by p we have

$$\left\{\frac{D}{p}\right\}=\left(\frac{D}{p}\right). \tag{4}$$

Let g be a primitive root of the prime p. For any integer D that is not divisible by p we have $D\equiv g^{\operatorname{ind}D} \pmod{p}$. Hence, in virtue of properties 1° and 2° of the symbol $\left\{\frac{D}{p}\right\}$, we have

$$\left\{\frac{D}{p}\right\}=\left\{\frac{g^{\operatorname{ind}D}}{p}\right\}=\left\{\frac{g}{p}\right\}^{\operatorname{ind}D} \tag{5}$$

Let $\left\{\frac{g}{p}\right\}=a$. Since $g^{p-1}\equiv 1 \pmod{p}$, by 1° and 2°, the equalities $a^{p-1}=\left\{\frac{g}{p}\right\}^{p-1}=\left\{\frac{g^{p-1}}{p}\right\}=\left\{\frac{1}{p}\right\}$ hold, but, in view of 2°, $\left\{\frac{1}{p}\right\}^2=\left\{\frac{1}{p}\right\}$, whence $\left\{\frac{1}{p}\right\}=0$ or $\left\{\frac{1}{p}\right\}=1$. We cannot have $\left\{\frac{1}{p}\right\}=0$ because, if that were the case then, by 2° (for $D'=1$), we would have $\left\{\frac{D}{p}\right\}=\left\{\frac{D}{p}\right\}\left\{\frac{1}{p}\right\}=0$, contrary to the assumption that $\left\{\frac{D}{p}\right\}$ is not identically equal to zero (if D is not divisible by p). Therefore $\left\{\frac{1}{p}\right\}=1$, and so $a^{p-1}=1$. But $a=\left\{\frac{g}{p}\right\}$ is a real number and the equation $x^{p-1}=1$, p being odd, has precisely two roots, 1 and -1. Consequently $a=1$ or $a=-1$. If $a=1$, then, by (5), for every integer D not divisible by p we have $\left\{\frac{D}{p}\right\}=1$, contrary to the assumption that $\left\{\frac{D}{p}\right\}$ is not identically equal to 1 (D not being divisible by p). Consequently, we must have $a=-1$, whence, by (5), we obtain $\left\{\frac{D}{p}\right\}=(-1)^{\operatorname{ind}D}$. So, by (2), $\left\{\frac{D}{p}\right\}=\left(\frac{D}{p}\right)$. The theorem is thus proved. It follows that any property of Legendre's symbol can be deduced from properties I and II and the fact that $\left(\frac{D}{p}\right)$ is not identically equal to 1 or to 0 for any odd prime p.

Formula (1) implies that

III. $\left(\dfrac{-1}{p}\right) = (-1)^{(p-1)/2}$.

In order to deduce some further properties of Legendre's symbol we prove the following

LEMMA OF GAUSS. $\left(\dfrac{D}{p}\right) = (-1)^{\lambda}$, *where* λ *is the number of the residues* mod p *that appear in the sequence*

$$D, 2D, 3D, \ldots, \tfrac{1}{2}(p-1)\,D \tag{6}$$

and that are greater than $p/2$.

PROOF. For $k = 1, 2, \ldots, (p-1)/2$, let r_k denote the remainder left by kD divided by p; we set $\varrho_k = r_r$ if $r_k < p/2$ or $\varrho_k = p - r_k$ if $r_k > p/2$. (The equality $r_r = p/2$ is impossible since, by assumption, p is an odd prime.)

Since D is not divisible by p and in sequence (6) the coefficients at D are natural numbers $\leqslant (p-1)/2$, neither the sum nor the difference of any two terms of sequence (6) is divisible by p. Hence it easily follows that the sum and the difference of any two different terms of the sequence

$$\varrho_1, \varrho_2, \ldots, \varrho_{\frac{p-1}{2}}, \tag{7}$$

are indivisible by p. But, according to the definition of numbers ϱ_k, they are all greater than zero and less than $(p-1)/2$ (because either $\varrho_k = r_k < p/2$, whence $2\varrho_k < p$, i.e. $2\varrho_k \leqslant p-1$, or $\varrho_k = p - r_k$ and $r_k > p/2$, whence $\varrho_k < p/2$ again). Since, by the property of the numbers of sequence (7) proved above, terms at different places are different, we infer that the numbers of (7) are (in a certain order) equal to the numbers $1, 2, \ldots, (p-1)/2$. Hence

$$\varrho_1\,\varrho_2 \cdots \varrho_{\frac{p-1}{2}} = \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\,D^{p-1} (\mathrm{mod}\, p), \tag{8}$$

the congruence being valid since, in view of the theorem of Fermat, $D^{p-1} \equiv 1 \ (\mathrm{mod}\ p)$.

Let λ_k be equal to 0 or 1 depending on whether $r_k < p/2$ or $r_k > p/2$. By the definition of number ϱ_k we have

$$\varrho_k \equiv (-1)^{\lambda_k} r_k (\mathrm{mod}\, p). \tag{9}$$

But, according to the definition of r_k, $r_k \equiv kD \pmod{p}$. Hence, in virtue of (9), we obtain

$$\varrho_1 \varrho_2 \cdots \varrho_{\frac{p-1}{2}} \equiv (-1)^{\lambda_1+\lambda_2+\dots+\lambda_{(p-1)/2}} \pmod{p}. \tag{10}$$

Formulae (8) and (9) together with the fact that the number $\left(\frac{p-1}{2}\right)!\,D^{(p-1)/2}$ is not divisible by p give

$$D^{\frac{p-1}{2}} \equiv (-1)^{\lambda_1+\lambda_2+\dots+\lambda_{(p-1)/2}} \pmod{p}. \tag{11}$$

But, according to the definition of λ_k, number $\lambda = \lambda_1+\lambda_2+\dots+\lambda_{(p-1)/2}$ is exactly the number of the remainders $> \frac{p}{2}$ obtained by dividing the numbers of (6) by p, successively. On the other hand, the left-hand side of (11) is congruent to $\left(\frac{D}{p}\right) \pmod{p}$. Consequently, (11) turns into the congruence $\left(\frac{D}{p}\right) \equiv (-1)^{\lambda} \pmod{p}$. To see that this in fact implies the equality $\left(\frac{D}{p}\right) = (-1)^{\lambda}$, asserted by the lemma, it is sufficient to note that $\left(\frac{D}{p}\right)$ is equal either to 1 or to -1 and that p, being an odd prime, is $\geqslant 3$. The lemma is thus proved. □

Numbers λ_k, defined in the course of the proof of the lemma of Gauss, are such that $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. In fact, if $r_k < p/2$, then $\lambda_k = 0$, and on the other hand, the definition of r_k shows that for an integer t_k the equality $kD = pt_k + r_k$ is valid, whence $2kD/p = 2t_k + 2r_k/p$ and, since $0 < 2r_k < p$, $[2kD/p] = 2t_k$, we have $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$. If $r_k > p/2$, then $1 < 2r_k/p < 2$ (because $r_k < p$), whence $[2r_k/p] = 1$ and $[2kD/p] = 2t_k + 1$. But, since for $r_k > p/2$ we have $\lambda_k = 1$, the formula $(-1)^{\lambda_k} = (-1)^{[2kD/p]}$ follows.

Since the formula proved above holds for any $k = 1, 2, \dots, (p-1)/2$, we have

$$(-1)^{\lambda} = (-1)^{\lambda_1+\lambda_2+\dots+\lambda_{(p-1)/2}} = (-1)^{\sum_{k=1}^{(p-1)/2}[2kD/p]}.$$

Thus the lemma of Gauss implies

COROLLARY. *We have*

$$\left(\frac{D}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}[2kD/p]}.$$

Consider the particular case of $D = 2$. By the corollary,

$$(12)\qquad \left(\frac{2}{p}\right) = (-1)^{\lambda} \quad \text{holds for} \quad \lambda = \sum_{k=1}^{(p-1)/2} [4k/p].$$

If $1 \leqslant k < p/4$, then $0 < 4k/p < 1$ and so $[4k/p] = 0$. The equality $k = p/4$ is impossible because p is odd. For $[p/4] < k \leqslant (p-1)/2$ we have $1 < 4k/p \leqslant 2(p-1)/p < 2$; consequently, $[4k/p] = 1$. From this we infer that among the summands of the sum for λ in (12) there are $(p-1)/2 - [p/4]$ summands equal to 1, the remaining ones being equal to zero. Consequently $\lambda = (p-1)/2 - [p/4]$. But, as is easy to verify, for odd p we have

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} \pmod 2.$$

In fact, number p, being odd, is equal to one of the following four numbers: $8k+1$, $8k+3$, $8k+5$, $8k+7$, where k is a natural number.

Write

$$f(p) = \frac{p-1}{2} - \left[\frac{p}{4}\right], \qquad g(p) = \frac{p^2-1}{8}.$$

Then, a simple calculation shows that

$$\begin{aligned}
&f(8k+1) = 4k-2k = 2k,\\
&f(8k+3) = 4k+1-2k = 2k+1,\\
&f(8k+5) = 4k+2-(2k+1) = 2k+1,\\
&f(8k+7) = 4k+3-(2k+1) = 2k+2,\\
&g(8k+1) = k(8k+2),\\
&g(8k+3) = (4k+1)(2k+1),\\
&g(8k+5) = (2k+1)(4k+3),\\
&g(8k+7) = (4k+3)(2k+2),
\end{aligned}$$

whence, in any case, $f(p) \equiv g(p) \pmod 2$. Consequently, $\lambda \equiv \frac{p^2-1}{8} \pmod 2$, and thus, by (12), we obtain property IV of Legendre's symbol:

$$\text{IV.}\quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

From this we infer that 2 is a quadratic residue to all primes p of the form $8k \pm 1$ and is not a quadratic residue to any prime p of the form $8k \pm 3$ (where k is an integer). Now we apply property IV in the proof of the following theorem:

THEOREM 1. *There exist infinitely many primes of the form* $8k-1$, *where* $k = 1, 2, \ldots$

PROOF. Let n be a natural number > 1. Number $N = 2(n!)^2 - 1$ is greater than 1 and has at least one odd prime divisor p which is not of the form $8k+1$. The reason is that if all the odd prime divisors of number N were of the form $8k+1$, then number N itself would be of this form, which is clearly impossible since N is of the form $8k-1$. We have $p \mid N$, i.e. $2(n!)^2 \equiv 1^2 (\bmod p)$, which proves that $2(n!)^2$ is a quadratic residue to the modulus p. Therefore $\left(\frac{2(n!)^2}{p}\right) = 1$, which, in view of property II, gives $\left(\frac{2(n!)^2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{n!}{p}\right)^2 = \left(\frac{2}{p}\right)$. Consequently, $\left(\frac{2}{p}\right) = 1$ and, in view of property IV, p must be of the form $8k \pm 1$. But the definition of p shows that p is not of the form $8k+1$, and so it must be of the form $8k-1$. But, since $p \mid N = 2(n!)^2 - 1$, we see that $p > n$. We have thus proved that for any natural number $n > 1$ there exists a prime p greater than n that is of the form $8k-1$. The proof is thus completed. □

THEOREM 2. *There exist infinitely many primes of the form* $8k+3$, *where* $k = 0, 1, 2, \ldots$

PROOF. Let n be a natural number > 1, and let $a = p_2 p_3 \ldots p_n$. Since a is odd, its square a^2 is of the form $8t+1$, number $N = a^2+2$ being of the form $8t+3$. If any prime divisor of N is of the form $8t \pm 1$, then number N itself is of this form, which is impossible. Therefore the odd number N has a (necessarily odd) prime divisor p which is not of the form $8k \pm 1$; consequently p is either of the form $8k+3$ or of the form $8k+5$. Suppose $p = 8k+5$. Since $p \mid N = a^2+2$, we have $a^2 \equiv -2 (\bmod p)$ and so $\left(\frac{-2}{p}\right) = 1$. But, in virtue of properties II, III, IV,

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8}.$$

Since $p = 8k+5$, number $\frac{1}{2}(p-1)$ is even and number $\frac{1}{8}(p^2-1)$ is odd, whence $\left(\dfrac{-2}{p}\right) = -1$, which is a contradiction. Therefore p cannot be of the form $8k+5$, and so it is of the form $8k+3$. But, since $p \mid a^2+2$, $a = p_2 p_3 \dots p_n$, we have $p > p_n$. Hence, since n may be chosen arbitrarily large, Theorem 2 is proved. □

THEOREM 3. *There exist infinitely many primes of the form* $8k+5$, *where* $k = 0, 1, 2, \dots$

PROOF. Let n be a natural number > 1 and let $a = p_2 p_3 \dots p_n$. Since a is an odd number, number $N = a^2+4$ is of the form $8k+5$. If any of its prime divisors is of the form $8t \pm 1$, then number N itself is of this form, but this is impossible. Consequently, N must have an odd prime divisor p which is either of the form $8k+3$ or of the form $8k+5$. The former case being impossible because, if $p = 8k+3$, the relation $p \mid N = a^2+4$ shows that $a^2 \equiv -4 \pmod{p}$, and so $\left(\dfrac{-4}{p}\right) = 1$; hence by properties II and III,

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2 = (-1)^{(p-1)/2}$$

whence, in view of $p = 8k+3$, we have $\left(\dfrac{-4}{p}\right) = -1$, which is a contradiction. Consequently, p is of the form $8k+5$. But, since $p \mid a^2+4$ and $a = p_2 p_3 \dots p_n$, we have $p > p_n$, which, in view of the fact that n is arbitrarily chosen, completes the proof of Theorem 3. □

2. The quadratic reciprocity law

Let p and q be two different odd primes.Consider the pairs (kq, lp), where $k = 1, 2, \dots, (p-1)/2$, $l = 1, 2, \dots, (q-1)/2$. The number of such pairs is clearly $\dfrac{p-1}{2} \cdot \dfrac{q-1}{2}$. For any of the pairs we have $kq \neq lp$ because, in the opposite case, i.e. if $kq = lp$, we have $p \mid kq$, whence, by $(p, q) = 1$, $p \mid k$, which is impossible because $k \leqslant (p-1)/2$. We divide all the pairs into two classes, one consisting of all the pairs for which $kq < lp$, the other comprising the pairs for which $kq > lp$. We calculate the number of pairs in each class as follows.

Given a number l out of the sequence $1, 2, \ldots, (q-1)/2$. If the pair (kq, lp) belongs to the first class, then $k < lp/q$. Since, as we know, lp/q is not an integer and since

$$\frac{lp}{q} \leqslant \frac{(q-1)p}{2q} \leqslant \frac{p}{2}, \quad \text{whence} \quad \left[\frac{lp}{q}\right] < \frac{p}{2},$$

we have

$$2\left[\frac{lp}{q}\right] < p, \quad \text{i.e.} \quad 2\left[\frac{lp}{q}\right] \leqslant p-1, \quad \text{whence} \quad \left[\frac{lp}{q}\right] \leqslant \frac{p-1}{2}.$$

Consequently, for a given number l, $l \leqslant \frac{1}{2}(q-1)$, k may take the values $1, 2, \ldots, \left[\frac{lp}{q}\right]$, which are $\left[\frac{lp}{q}\right]$ in number. From this we infer that the number of pairs which belong to the first class is $\sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]$. Similarly, the number of the pairs that belong to the second class is $\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]$. Since the number of all the pairs in both classes is $\frac{p-1}{2}\cdot\frac{q-1}{2}$, we obtain the equality

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right] + \sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]. \tag{13}$$

In virtue of the corollary to the lemma of Gauss, by properties I and II we have

$$\left(\frac{2q}{p}\right) = \left(\frac{2(p+q)}{p}\right) = \left(\frac{2^2\,\frac{q+p}{2}}{p}\right) = \left(\frac{(q+p)/2}{p}\right)$$

$$= (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{k(p+q)}{p}\right]} = (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \sum_{k=1}^{(p-1)/2} k} = (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right] + \frac{p^2-1}{8}}$$

(the last equality being valid since $\sum_{k=1}^{(p-1)/2} k = \frac{1}{8}(p^2-1)$). But (since q is odd), in virtue of II and IV we have

$$\left(\frac{2q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p^2-1}{8}},$$

which, combined with the formula proved above for $\left(\frac{2q}{p}\right)$, implies the equality

$$\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]}$$

valid for any odd p and q. Hence

$$\left(\frac{p}{q}\right) = (-1)^{\sum\limits_{l=1}^{(q-1)/2}\left[\frac{lp}{q}\right]}$$

By (13), these two formulae show that the formula

$$\text{V.}\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

is valid for any two different odd primes p and q. This formula is known under the name of the *quadratic reciprocity law*.

Number $\frac{p-1}{2}\cdot\frac{q-1}{2}$ is odd if and only if each of the numbers p and q is of the form $4k+3$; hence equality V may be expressed by saying:

if two different odd primes p and q are of the form $4k+3$, *then* $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$; *if at least one of them is of the form* $4k+1$, *then* $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

There are as many as seven different proofs of the law of quadratic reciprocity given only by Gauss himself. A table of 45 proofs of this law, ordered according to the time of their discovery (from 1796 to 1897), is given by P. Bachmann [2], p. 203. The number of proofs has considerably increased since then.

Now we are going to apply property V to the proof of

THEOREM 4. *There are infinitely many primes of the form* $5k-1$, *where k is a natural number.*

PROOF. Let n be an arbitrary natural number > 1. Let $N = 5(n!)^2 - 1$. Clearly, N is an odd number > 1 and, since it is not of the form $5t+1$, it has at least one prime divisor p which is odd (different from 5) and not of the form $5t+1$. We have $p > n$. Since $p \mid N$, we have $5(n!)^2 \equiv 1 \pmod{p}$, whence $\left(\frac{5}{p}\right) = 1$. By V, we thus have $\left(\frac{p}{5}\right) = 1$. The prime p, different from 5, must be of the form $5k\pm 1$ or $5k\pm 2$. If $p = 5k\pm 2$, then, by I and II, $\left(\frac{p}{5}\right) = \left(\frac{\pm 2}{5}\right) = \left(\frac{\pm 1}{5}\right)\left(\frac{2}{5}\right)$. But since, by III, $\left(\frac{\pm 1}{5}\right) = 1$ and, by IV, $\left(\frac{2}{5}\right) = -1$, we obtain $\left(\frac{p}{5}\right) = -1$, which is a contradiction. Therefore number p must be of the form $5k\pm 1$, and so, since it is proved not to be of the form $5k+1$, it is of the form $5k-1$. Thus we have shown that for any natural number n there exists a prime $p > n$ that is of the form $5k-1$. This completes the proof of the theorem. ☐

If $p = 5k-1$ (k being a natural number) is a prime, then k must be even (since otherwise p would be an even number > 2, and thus composite). Therefore $k = 2t$, where t is a natural number and $p = 10t-1$. From Theorem 4 we infer that *there exist infinitely many primes of the form* $10t-1$, *where t is a natural number*. In other words, there exist infinitely many primes whose last digits are 9.

It is easy to verify that there exist infinitely many primes of the form $5k\pm 2$, where k is a natural number. In fact, let n be an arbitrary natural number > 2. We put $N = p_2 p_3 \dots p_n - 2$. Then N is an odd number > 1 whose prime divisors are different from 5. If all its prime divisors were of the form $5k\pm 1$, number N itself would be of this form. Consequently, there exists at least one prime divisor p of N which is different from 5 and not of the form $5k\pm 1$. So p must be of the form $5k\pm 2$. But, since $p > p_n$, the theorem follows. The theorem on arithmetical progressions implies that there are infinitely many primes of the forms $5k+2$ and $5k-2$. The proof, however, is far more difficult. Since k must be an odd number, one easily sees that the former of the two theorems is equivalent to the theorem stating that there exist infinitely many primes whose last digits are 7; the latter theorem is equivalent to the theorem stating that there exist infinitely many primes whose last digits are 3.

THEOREM 5. *Every prime p which is of the form $6k+1$ is of the form $p = 3x^2 + y^2$, where x, y are natural numbers.*

PROOF. Suppose that p is a prime of the form $6k+1$. By property V of Legendre's symbol, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. By property I, $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Combining these two equalities, we obtain

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1,$$

which proves that -3 is a quadratic residue to the modulus p. Therefore there exists an integer a such that $a^2+3 \equiv 0 \pmod{p}$. In view of Thue's theorem (see Chapter I, § 13), there exist natural numbers x, y, each $\leqslant \sqrt{p}$, such that for a suitable choice of the sign the number $ax \pm y$ is divisible by p. Hence it follows that $p \mid a^2x^2-y^2$. But, since $p \mid a^2+3$, whence $p \mid a^2x^2+3x^2$, we have $p \mid 3x^2+y^2$. But $x \leqslant \sqrt{p}$ and $y \leqslant \sqrt{p}$. Consequently, in view of the fact that p is a prime, we have $x^2 < p$ and $y^2 < p$, whence $3x^2+y^2 < 4p$. In virtue of the relation $p \mid 3x^2+y^2$, we then have $3x^2+y^2 = pt$, where t is a natural number < 4. If $t = 3$, then $3 \mid y$ and so $y = 3z$, where z is a natural number, whence $p = x^2+3z^2$. If $t = 2$, then the numbers x, y must both be even or both be odd. In either case number $2p = 3x^2+y^2$ is divisible by 4, whence $2 \mid p$, which is impossible. In the case where $t = 1$, we have $p = 3x^2+y^2$. Theorem 5 is thus proved. ☐

It is easy to prove that if a prime p is of the form $p = 3x^2+y^2$, where x, y are natural numbers, then p must be of the form $p = 6k+1$, where k is a natural number. From Theorem 10 of Chapter V it follows that any prime of the form $6k+1$ has exactly one representation in the form $3x^2+y^2$, where x and y are natural numbers. B. van der Pol and P. Speziali [1] have tabulated the representations in the form $3x^2+y^2$ of primes of the form $6k+1$ which are less than 10000. In particular, we have
$7 = 3\cdot 1^2+2^2$, $13 = 3\cdot 2^2+1^2$, $19 = 3\cdot 1^2+4^2$, $31 = 3\cdot 3^2+2^2$,
$37 = 3\cdot 2^2+5^2$, $43 = 3\cdot 3^2+4^2$, $61 = 3\cdot 2^2+7^2$, $67 = 3\cdot 1^2+8^2$,
$73 = 3\cdot 4^2+5^2$, $79 = 3\cdot 5^2+2^2$, $97 = 3\cdot 4^2+7^2$.

As has been noticed by A. Mąkowski, Theorem 5 implies the following corollary: *for any prime p of the form $6k+1$ number $2p^4$ is the sum of three positive biquadrates.*

This is obtained immediately from Theorem 5 by a simple application of the identity

$$2(3x^2+y^2)^4 = (3x^2+2xy-y^2)^4+(3x^2-2xy-y^2)^4+(4xy)^4$$

and by the remark that for $p = 3x^2+y^2$ we have the equality $3x^2 \pm 2xy - y^2 = p-2y^2 \pm 2xy$ the right-hand side of which is different from zero since $p = 6k+1$ is odd.

We note that also the following identity holds:

$$2(3x^2+y^2)^2 = (3x^2+2xy-y^2)^2+(3x^2-2xy-y^2)^2+(4xy)^2.$$

Hence, in particular, for $x = 1$, $y = 2$ we obtain

$$2\cdot 7^4 = 3^4+5^4+8^4, \qquad 2\cdot 7^2 = 3^2+5^2+8^2,$$

and, for $x = 2$, $y = 1$, we find

$$2\cdot 13^4 = 15^4+7^4+8^4, \qquad 2\cdot 13^2 = 15^2+7^2+8^2.$$

In this connection, we present the following two identities:

$$2(3x^2+y^2)^2 = (x+y)^4+(x-y)^4+(2x)^4,$$
$$2(3x^2+y^2) = (x+y)^2+(x-y)^2+(2x)^2.$$

From them we derive the following corollary: *for any prime p of the form $6k+1$ number $2p^2$ is a sum of three biquadrates of natural numbers.*

For example, for $x = 1$, $y = 2$, we have

$$2\cdot 7^2 = 3^4+1^4+2^4, \qquad 2\cdot 7 = 3^2+1^2+2^2;$$

for $x = 2$, $y = 1$ we have

$$2\cdot 13^2 = 3^4+1^4+4^4, \qquad 2\cdot 13 = 3^2+1^2+4^2.$$

3. Calculation of Legendre's symbol by its properties

The five properties of Legendre's symbol deduced from its definition combined with the fact that the value of the symbol is either 1 or -1 enable us to calculate its value.

Let p be a given odd prime and D an integer not divisible by p. Let r be the remainder left by D divided by p. Consequently, we have $0 < r < p$, and, by property I, $\left(\frac{D}{p}\right) = \left(\frac{r}{p}\right)$. Let a^2 denote the greatest square that divides r. We have $r = ka^2$, where either $k = 1$ or k is the product of different primes, i.e. $k = q_1 q_2 \dots q_s$, with $q_1 < q_2 \dots < q_s$; moreover, since $r < p$, we have $q_s < p$. In virtue of property II we have

$$\left(\frac{D}{p}\right) = \left(\frac{ka^2}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{a}{p}\right)^2 = \left(\frac{k}{p}\right),$$

this being equal to $\left(\frac{1}{p}\right) = 1$ or to $\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\dots\left(\frac{q_s}{p}\right)$. If $q_1 = 2$, then $\left(\frac{q_1}{p}\right)$ is calculated by the use of property IV. If $q_1 > 2$, then the values of the symbols $\left(\frac{q}{p}\right)$, where q and p are odd primes and $q < p$, are still to be calculated. By property V, we have

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Thus the calculation of Legendre's symbol $\left(\frac{D}{p}\right)$ reduces to the calculation of the symbols $\left(\frac{D'}{q}\right)$, where q is an odd prime less than p.

Therefore, after a finite number of reductions, we obtain the value of the symbol $\left(\frac{D}{p}\right)$. This procedure has the disadvantage that it involves expansions into prime factors. In order to avoid that, Jacobi introduced a more general symbol; it will be investigated in the next section.

4. Jacobi's symbol and its properties

Jacobi defined the symbol $\left(\frac{D}{P}\right)$ for odd numbers $P > 1$ and integers D relatively prime to P as follows:

If $P = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ is the factorization of P into prime factors (each factor being odd), then

$$\left(\frac{D}{P}\right) = \left(\frac{D}{q_1}\right)^{\alpha_1}\left(\frac{D}{q_2}\right)^{\alpha_2}\dots\left(\frac{D}{q_s}\right)^{\alpha_s}, \tag{14}$$

where on the right-hand side we have Legendre's symbols.

It follows immediately from the definition that if P is a prime, then Jacobi's symbol is equal to Legendre's symbol. However, for investigating the quadratic residuacity Jacobi's symbol does not correspond exactly to Legendre's symbol. The reason is that though the equality $\left(\frac{D}{P}\right) = -1$ implies that D is not a quadratic residue to P because then at least one of the factors $\left(\frac{D}{q_i}\right)$, one on the right-hand side of (14), must be equal to -1, whence the congruence $x^2 \equiv D \pmod{q_i}$ is insolvable, and so, *a fortiori* (since $q_i \mid P$) the congruence $x^2 \equiv D \pmod{P}$ is insolvable, the relation $\left(\frac{D}{P}\right) = +1$ does not necessarily imply that D is a quadratic residue to P, for example $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ and the congruence $x^2 \equiv 2 \pmod{15}$ is insolvable because the congruence $x^2 \equiv 2 \pmod 3$ is insolvable.

Jacobi's symbol possesses five properties similar to those of Legendre's symbol. In order to prove them we note that (14) may be rewritten in the form

$$\left(\frac{D}{P}\right) = \left(\frac{D}{q_1}\right)\left(\frac{D}{q_2}\right)\cdots\left(\frac{D}{q_s}\right), \tag{15}$$

where $P = q_1 q_2 \ldots q_s$ and the primes $q_1, q_2, \ldots, q_s$ are not necessarily different.

PROPERTY I. *If* $D \equiv D' \pmod P$, *then* $\left(\frac{D}{P}\right) = \left(\frac{D'}{P}\right)$.

PROOF. In virtue of (15) we have

$$\left(\frac{D}{P}\right) = \left(\frac{D}{q_1}\right)\left(\frac{D}{q_2}\right)\cdots\left(\frac{D}{q_s}\right); \quad \left(\frac{D'}{P}\right) = \left(\frac{D'}{q_1}\right)\cdots\left(\frac{D'}{q_s}\right). \tag{16}$$

If $D \equiv D' \pmod P$, then, *a fortiori*, $D \equiv D' \pmod{q_i}$ for any $i = 1, 2, \ldots, s$. Consequently, by property I of Legendre's symbol, $\left(\frac{D}{q_i}\right) = \left(\frac{D'}{q_i}\right)$ for $i = 1, 2, \ldots, s$, whence, by (16), $\left(\frac{D}{P}\right) = \left(\frac{D'}{P}\right)$. □

PROPERTY II. $\left(\frac{DD'}{P}\right) = \left(\frac{D}{P}\right)'\left(\frac{D'}{P}\right)$ *for any integers D and D' not divisible by P.*

The proof follows easily from property II of Legendre's symbol, formula (16) and the fact that

$$\left(\frac{DD'}{P}\right) = \left(\frac{DD'}{q_1}\right)\left(\frac{DD'}{q_2}\right)\cdots\left(\frac{DD'}{q_s}\right).$$

As an immediate consequence of property II we obtain $\left(\frac{1}{P}\right) = 1$.

PROPERTY III. $\left(\dfrac{-1}{P}\right) = (-1)^{(P-1)/2}$.

PROOF. In view of (15), by property III of Legendre's symbol, we have

$$(17)\quad \left(\frac{-1}{P}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{-1}{q_2}\right)\dots\left(\frac{-1}{q_s}\right) = (-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}+\dots+\frac{q_s-1}{2}}.$$

Consider the identity

$$P = q_1 q_2 \cdots q_s = \big((q_1-1)+1\big)\big((q_2-1)+1\big)\dots\big((q_s-1)+1\big).$$

All the numbers q_1-1, q_2-1, ..., q_s-1 are even; consequently the product of any two of them is divisible by 4. Hence

$$P = 4k+1+(q_1-1)+(q_2-1)+\dots+(q_s-1),$$

and so

$$\frac{P-1}{2} = 2k+\frac{q_1-1}{2}+\frac{q_2-1}{2}+\dots+\frac{q_s-1}{2}.$$

Therefore

$$(-1)^{\frac{P-1}{2}} = (-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}+\dots+\frac{q_s-1}{2}}.$$

Hence, by (17), property III follows. □

PROPERTY IV. $\left(\dfrac{2}{P}\right) = (-1)^{(P^2-1)/8}$.

PROOF. In virtue of (15), by property IV of Legendre's symbol, we have

$$(18)\quad \left(\frac{2}{P}\right) = \left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right)\dots\left(\frac{2}{q_s}\right) = (-1)^{\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\dots+\frac{q_s^2-1}{8}}.$$

Since the square of any odd natural number is of the form $8k+1$, the identity

$$P^2 = \big((q_1^2-1)+1\big)\big((q_2^2-1)+1\big)\dots\big((q_s^2-1)+1\big)$$

shows that any of the differences q_1^2-1, q_2^2-1, ..., q_s^2-1 is divisible by 8. Consequently, the product of any two of them is divisible by 64. Hence

$$P^2 = 64k+1+(q_1^2-1)+(q_2^2-1)+\dots+(q_s^2-1),$$

and so

$$\frac{P^2-1}{8} = 8k+\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\dots+\frac{q_s^2-1}{8},$$

whence

$$(-1)^{\frac{P^2-1}{8}} = (-1)^{\frac{q_1^2-1}{8}+\frac{q_2^2-1}{8}+\dots+\frac{q_s^2-1}{8}},$$

which, by (18), completes the proof of property IV. □

PROPERTY V. $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$ *for any relatively prime odd numbers* $P, Q > 1$.

PROOF. Let $Q = r_1 r_2 \dots r_t$, where $r_1, r_2, \dots, r_t$ are not necessarily different odd primes.

In virtue of (15), property II, and property V of Legendre's symbol, we have

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{s}\prod_{j=1}^{t}\left(\frac{q_i}{r_j}\right)\left(\frac{r_j}{q_i}\right) = (-1)^{\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{q_i-1}{2}\cdot\frac{r_j-1}{2}}. \tag{19}$$

But

$$\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{q_i-1}{2}\cdot\frac{r_j-1}{2} = \sum_{i=1}^{s}\frac{q_i-1}{2}\cdot\sum_{j=1}^{t}\frac{r_j-1}{2}. \tag{20}$$

As is easily noticed, in the proof of property III

$$\sum_{i=1}^{s}\frac{q_i-1}{2} = \frac{P-1}{2} - 2k \quad \text{and similarly} \quad \sum_{j=1}^{t}\frac{r_j-1}{2} = \frac{Q-1}{2} - 2l,$$

whence, P and Q being odd, we have

$$\sum_{i=1}^{s}\frac{q_i-1}{2}\cdot\sum_{j=1}^{t}\frac{r_j-1}{2} = \frac{P-1}{2}\cdot\frac{Q-1}{2} + 2h.$$

This by (19) and (20) completes the proof of property V. □

5. Eisenstein's rule

The properties of Jacobi's symbol introduced in the preceding section will serve to obtain the Eisenstein rule, by means of which the value of Jacobi's symbol (and thus also of Legendre's symbol) may be calculated without using the factorization of a number into primes.

First of all we note that the task of calculating the value of $\left(\frac{D}{P}\right)$, where P is an odd number > 1 and D an integer relatively prime to P, may be reduced to that of calculating the value of $\left(\frac{Q}{P}\right)$, where Q is an odd natural number. In fact if 2^β (where β is an integer $\geqslant 0$) is the greatest power of 2 that divides D, then $D = (-1)^\alpha 2^\beta Q$, where $\alpha = 0$ or 1, Q being a natural odd number. Clearly, in order to find the number Q we do not need to know the factorization of D into primes; it is sufficient to divide D by consecutive powers of 2.

By the properties of Jacobi's symbol, in virtue of the formula for D, we obtain

$$\left(\frac{D}{P}\right) = (-1)^{\frac{P-1}{2}\alpha + \frac{P^2-1}{8}\beta}\left(\frac{Q}{P}\right).$$

Thus it remains to find the value of $\left(\frac{Q}{P}\right)$, where Q, P are odd relatively prime natural numbers.

Let R be the remainder left by Q divided by P. Consequently, R is one of the numbers of the sequence $1, 2, \ldots, P-1$. Number $P-R$ also belongs to this sequence. Hence, for an integer t we have

$$Q = Pt+R \quad \text{and} \quad Q = P(t+1)-(P-R).$$

Since the sum of the numbers R and $P-R$ is odd, one of them must be odd, the other being even. Let P_1 denote the odd number. If $P_1 = R$, then $Q = Pt+P_1$; if $P_1 = P-R$, then $Q = P(t+1)-P_1$. In any case $Q = Pk+\varepsilon_1 P_1$, where k is an integer and ε_1 is 1 or -1. We note that k must be an even number, since otherwise the number $Q \pm P_1$ would be odd, which is clearly impossible because the numbers Q and P_1 are odd. Consequently, $k = 2k_1$, where k_1 is an integer. We have $Q = 2k_1 P + \varepsilon_1 P_1$.

If $P_1 \neq 1$, then we may repeat the above reasoning with P and P_1 in place of Q and P. Then we obtain the equality $P = 2k_2 P_1 + \varepsilon_2 P_2$, where k_2 is an integer and $\varepsilon_2 = \pm 1$, P_2 is an odd natural number.

If $P_2 \neq 1$, then, as in the previous case, $P_1 = 2k_3 P_2 + \varepsilon_3 P_3$ and so on. Numbers $P, P_1, P_2, \ldots$ are strictly decreasing because $P_1 \leqslant P-1$, $P_2 \leqslant P_1 - 1, \ldots$ Therefore the sequence of the equalities that link together numbers $P, P_1, P_2, \ldots$ cannot be infinite because the number of odd natural numbers $< P$ is finite. Therefore we ultimately obtain the last equality, $P_{n-2} = 2k_n P_{n-1} + \varepsilon_n P_n$, where P_n must be equal to 1, since otherwise a next equality could be obtained. Thus we obtain the sequence of equalities:

$$\begin{gathered} Q = 2k_1 P + \varepsilon_1 P_1, \quad P = 2k_2 P_1 + \varepsilon_2 P_2, \quad P_1 = 2k_3 P_2 + \varepsilon_3 P_3, \quad \ldots, \\ P_{n-3} = 2k_{n-1} P_{n-2} + \varepsilon_{n-1} P_{n-1}, \quad P_{n-2} = 2k_n P_{n-1} + \varepsilon_n P_n, \end{gathered} \tag{21}$$

where $P_n = 1$.

The first equality of (21), by properties I and II of Jacobi's symbol, gives

$$\left(\frac{Q}{P}\right) = \left(\frac{\varepsilon_1}{P}\right)\left(\frac{P_1}{P}\right). \tag{22}$$

If $\varepsilon_1 = 1$, then

$$\left(\frac{\varepsilon_1}{P}\right) = 1 = (-1)^{\frac{P-1}{2}\cdot\frac{1-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}};$$

if $\varepsilon_1 = -1$, then

$$\left(\frac{\varepsilon_1}{P}\right) = (-1)^{\frac{P-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}.$$

In any case we then have

$$\left(\frac{\varepsilon_1}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}}.$$

In virtue of property V of Jacobi's symbol and by the fact that the square of Jacobi's symbol is always equal to 1, we have

$$\left(\frac{P_1}{P}\right) = \left(\frac{P}{P_1}\right)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{P_1-1}{2}},$$

whence, by (22),

$$\left(\frac{Q}{P}\right) = \left(\frac{P}{P_1}\right)\cdot(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{P_1-1}{2}}.$$

But (since $\varepsilon_1^2 = 1$) we have

$$\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2} + \frac{P-1}{2}\cdot\frac{P_1-1}{2} = \frac{P-1}{2}\cdot\frac{P_1-\varepsilon_1}{2} = \frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1 - \varepsilon_1^2}{2\varepsilon_1} =$$

$$= \frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1 - 1}{2\varepsilon_1}.$$

Moreover, trivially, $(-1)^{a/\varepsilon_1} = (-1)^a$ for $\varepsilon_1 = \pm 1$, and so

$$(-1)^{\frac{P-1}{2}\cdot\frac{1-\varepsilon_1}{2}+\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}};$$

consequently

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}}\left(\frac{P}{P_1}\right).$$

Similarly, from the second equality of (20) we find

$$\left(\frac{P}{P_1}\right)=(-1)^{\frac{P_1-1}{2}\cdot\frac{\varepsilon_2 P_2-1}{2}}\left(\frac{P_1}{P_2}\right)$$

and so on. Finally, the last but one equality gives

$$\left(\frac{P_{n-3}}{P_{n-2}}\right)=(-1)^{\frac{P_{n-2}-1}{2}\cdot\frac{\varepsilon_{n-1} P_{n-1}-1}{2}}\left(\frac{P_{n-2}}{P_{n-1}}\right)$$

and from the last equality, taking into account that $P_n = 1$, we find

$$\left(\frac{P_{n-2}}{P_{n-1}}\right)=\left(\frac{\varepsilon_n}{P_{n-1}}\right).$$

But hence, for $\varepsilon_n = \pm 1$, we easily obtain

$$\left(\frac{\varepsilon_n}{P_{n-1}}\right)=(-1)^{\frac{P_{n-1}-1}{2}\frac{\varepsilon_n-1}{2}},$$

whence, in view of $P_n = 1$, we obtain

$$\left(\frac{P_{n-2}}{P_{n-1}}\right)=(-1)^{\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_n P_n-1}{2}}.$$

Now if we put together the formulae obtained for $\left(\frac{Q}{P}\right)$, $\left(\frac{P}{P_1}\right)$, ..., $\left(\frac{P_{n-2}}{P_{n-1}}\right)$ we get the final formula

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}+\frac{P_1-1}{2}\cdot\frac{\varepsilon_2 P_2-1}{2}+\dots+\frac{P_{n-1}-1}{2}\cdot\frac{\varepsilon_n P_n-1}{2}}.$$

The value of the right-hand side of this equality depends on the number of odd summands in the exponent. The product $\frac{P-1}{2}\cdot\frac{\varepsilon_1 P_1-1}{2}$ is odd if and only if each of the numbers P and $\varepsilon_1 P_1$ is of the form $4t+3$. Therefore we may write

$$\left(\frac{Q}{P}\right)=(-1)^m, \tag{23}$$

where number m is equal to the number of those of the pairs P_{i-1}, $\varepsilon_i P_i$ ($i = 1, 2, ..., n$, and $P_0 = P$) in which both P_{i-1} and $\varepsilon_i P_i$ are of the form $4t+3$. This gives

EISENSTEIN'S RULE. *To calculate* $\left(\frac{Q}{P}\right)$ *we look at equalities* (21) *and find the number m of the pairs* P_{i-1} *and* $\varepsilon_i P_i$ *in which both* P_{i-1} *and* $\varepsilon_i P_i$ *are of the form* $4t+3$. *Then we substitute m in* (23).

As is easy to see, the rule makes it possible to calculate the value of Jacobi's symbol without developing a number into prime factors.

EXAMPLES. 1. We apply Eisenstein's rule in order to find the value of $\left(\frac{641}{257}\right)$. Here equalities (21) are the following:

$$641 = 2\cdot 257+127,\qquad 257 = 2\cdot 127+3,\qquad 127 = 42\cdot 3+1.$$

Among the pairs 257, 127; 127, 3; 3, 1, only the second is such that each of its terms is of the form $4t+3$. Therefore $m = 1$, and, consequently, $\left(\frac{641}{257}\right) = -1$, which shows that number 641 is not a quadratic residue for the modulus 257.

2. We calculate the value of the symbol $\left(\frac{65537}{274177}\right)$. We have $65537 = 0\cdot 274177 +65537$, $274177 = 4\cdot 65537+12029$, $65537 = 6\cdot 12029-6637$, $12029 = 2\cdot 6637-1245$, $6637 = 6\cdot 1245-833$, $1245 = 2\cdot 833-421$, $833 = 2\cdot 421-9$, $421 = 46\cdot 9+7$, $9 = 2\cdot 7 -5$, $7 = 2\cdot 5-3$, $5 = 2\cdot 3-1$.

Among the pairs P_{i-1}, $\varepsilon_i P_i$ only in the pairs 7, -5 and 3, -1 both of the terms are of the form $4t+3$. Therefore $m = 2$, whence $\left(\frac{65537}{274177}\right) = 1$.

3. In order to calculate the value of $\left(\frac{-104}{997}\right)$ we find that $-104 = (-1)\cdot 2^3\cdot 13$. So $\left(\frac{-104}{997}\right) = \left(\frac{-1}{997}\right)\left(\frac{2}{997}\right)\left(\frac{13}{997}\right)$. Number 997 is of the form $4t+1$, so $\left(\frac{-1}{997}\right) = 1$. Number 997 is of the form $8t+5$, so $\left(\frac{2}{997}\right) = -1$. Therefore $\left(\frac{-104}{997}\right) = -\left(\frac{13}{997}\right)$. In order to calculate the value of $\left(\frac{13}{997}\right)$ we write equalities like (20), i.e.

$$13 = 0\cdot 997+13,\qquad 997 = 76\cdot 13+9,\qquad 13 = 2\cdot 9-5,\qquad 9 = 2\cdot 5-1.$$

We see that there is no pair P_{i-1}, $\varepsilon_i P_i$ in which both terms are of the form $4t+3$. Consequently, $m = 0$, whence $\left(\frac{13}{997}\right) = 1$ and so $\left(\frac{-104}{997}\right) = -1$.

CHAPTER X

MERSENNE NUMBERS AND FERMAT NUMBERS

1. Some properties of Mersenne numbers

Mersenne numbers $M_n = 2^n - 1$ have already been discussed; cf. Chapter IV, § 5. Theorem 5 of Chapter V may be expressed by saying that in order that an even number should be a perfect number it is necessary and sufficient that it should be of the form $2^{n-1}M_n$, where n is a natural number and M_n is a Mersenne prime number. This is why Mersenne numbers which are prime are of particular interest; moreover, the greatest prime numbers that are known are Mersenne numbers.

As we learned in Chapter IV, § 5, if a Mersenne number M_n is prime, number n is also prime; the converse, however, is not necessarily true (for example $M_{11} = 23 \cdot 89$).

It is easy to prove that a natural number m is a Mersenne number if and only if $m+1$ has no odd prime divisor. As noticed by Golomb [1], this provides a method of finding all Mersenne numbers, the method being similar to the sieve of Eratosthenes.

We now prove a theorem which, in a number of cases, enables us to decide whether a Mersenne number is composite or not.

THEOREM 1. *If q is a prime of the form $8k+7$, then $q \mid M_{(q-1)/2}$.*

PROOF. In virtue of a formula of Chapter IX, since q is a prime, we have $\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \pmod{q}$. If q is a prime of the form $8k+7$, then, by property IV of Legendre's symbol (cf. Chapter IX, § 1), we have $\left(\frac{2}{q}\right) = 1$. Consequently, $2^{(q-1)/2} \equiv 1 \pmod{q}$, whence $q \mid 2^{(q-1)/2} - 1$, as required. □

An easy induction shows that $2^{4k+3} > 8(k+1)$. In fact, $2^7 > 8 \cdot 2$, and, if $2^{4k+3} > 8(k+1)$, then $2^{4(k+1)+3} > 2^4 \cdot 8(k+1) > 8(k+2)$. Therefore, if $q = 8k+7 > 7$, then $2^{(q-1)/2} - 1 > 8k+7 = q$, which proves that *if q is* *a prime of the form* $8k+7>7$, *then the number* $M_{(q-1)/2}$ *is composite — it is divisible by* q. Hence the following

COROLLARY. *If* n *is a prime* >3 *of the form* $4k+3$ *and if number* $q=2n+1$ *is a prime, then number* M_n *is composite; for, it is divisible by* q.

In particular, this is the way to establish that the following Mersenne numbers are composite, a prime divisor of any of them being also found: $23\mid M_{11}$, $47\mid M_{23}$, $167\mid M_{83}$, $263\mid M_{131}$, $359\mid M_{179}$, $383\mid M_{191}$, $479\mid M_{239}$, $503\mid M_{251}$, $719\mid M_{359}$, $839\mid M_{419}$, $863\mid M_{431}$, $887\mid M_{443}$, $983\mid M_{491}$, $1319\mid M_{659}$, $1367\mid M_{683}$, $1439\mid M_{719}$, $1487\mid M_{743}$, $1823\mid M_{911}$, $2039\mid M_{1019}$.

It follows from the Conjecture H (Chapter III, § 8) that there exist infinitely many prime numbers p of the form $4k+3$ for which $q=2p+1$ is a prime. Thus, by the corollary, we see that the Conjecture H implies the existence of infinitely many primes p such that the numbers M_p are composite (cf. Schinzel and Sierpiński [3], p. 198, C_9).

As regards Theorem 1, we note that an argument analogous to the one used in its proof shows that, *if* q *is a prime of the form* $8k+1$, *then* $q\mid M_{(q-1)/2}$. Here, however, the number $(q-1)/2=4k$ cannot be a prime. For example, we have $17\mid M_8$, $41\mid M_{20}$, $89\mid M_{44}$, $97\mid M_{48}$.

We do not know any composite Mersenne number which has a prime index and which is not a product of different primes. Neither are we able to prove that there exist infinitely many square-free Mersenne numbers.

THEOREM 2. *If* n *is a natural number* >1, *then* M_n *cannot be the m-th power of a natural number, m being a natural number* >1 (cf. Gerono [1]).

PROOF. Suppose that $2^n-1=k^m$, where k and $m>1$ are natural numbers. Since $n>1$, number k is odd. If m were even, then k^m would be of the form $8t+1$, whence $k^m+1=2(4t+1)$. But, since $n>1$, $k^m+1=2^n$ is divisible by 4, which is a contradiction. Consequently m is odd and $2^n=k^m+1=(k+1)(k^{m-1}-k^{m-2}+\ldots-k+1)$, the second of the factors being an algebraic sum of an odd number of odd summands, is an odd number, whence, in virtue of the fact that it is a divisor of 2^n, it is equal to 1. Therefore $2^n=k+1$, and so $m=1$, contrary to the assumption. This proves Theorem 2. □

Theorem 2 implies that there are no Mersenne numbers that are squares except $M_1 = 1^2$. On the other hand, there exist Mersenne numbers which are triangular numbers. However, there are only four of them $M_1 = t_1$, $M_2 = t_2$, $M_4 = t_5$, $M_{12} = t_{90}$ (cf. Ramanujan [1], Nagell [4], [12] and Hasse [2]).

It is easy to prove that for $|x| < \frac{1}{2}$ the following equality holds:

$$\frac{1}{(1-x)(1-2x)} = M_1 + M_2 x + M_3 x^2 + \dots$$

EXERCISES. 1. Prove that every odd natural number is a divisor of infinitely many Mersenne numbers.

PROOF. If m is an odd natural number, then by the theorem of Euler, for any natural number k we have $m \mid M_{k\varphi(m)}$. □

2. Find the least Mersenne number that is divisible by the square of a natural number > 1.

ANSWER. It is the number $M_6 = 2^6 - 1 = 63 = 3^2 \cdot 7$, because $M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15 = 3 \cdot 5$ and $M_5 = 31$.

3. Find the least Mersenne number which has an odd index and which is divisible by the square of a natural number > 1.

ANSWER. It is the number $M_{21} = 7^2 \cdot 127 \cdot 337$ because $M_7 = 127$, $M_9 = 7 \cdot 73$, $M_{11} = 23 \cdot 89$, $M_{13} = 8191$, $M_{15} = 7 \cdot 31 \cdot 151$, $M_{17} = 131071$, $M_{19} = 524287$.

REMARK. The next Mersenne number after M_{21} which has odd index and is divisible by the square of a natural number > 1 is the number M_{63}; the next number with the same property is M_{105}. They are both divisible by 7^2 because $M_{21} \mid M_{63}$ and $M_{21} \mid M_{105}$.

4. Prove that if a and n are natural numbers greater than 1, then, if $a^n - 1$ is a prime, it is a Mersenne number.

PROOF. In the case where $a > 2$, we have $a - 1 \mid a^n - 1$, so, in view of $n > 1$, $1 < a - 1 < a^n - 1$, which shows that number $a^n - 1$ cannot be a prime. Thus we see that the assumption that $a^n - 1$ is a prime implies that $a \leqslant 2$, whence $a = 2$ (because $1 - 1$ is not a prime). Consequently, $a^n - 1 = M_n$. □

5. Prove that, if m is an arbitrary natural number, s the number of digits of m in the scale of ten, then there exists a Mersenne number M_n whose first s digits are equal to the s digits of m, respectively.

The proof follows immediately from an analogous property of the numbers 2^n (cf. Sierpiński [11], theorem 2).

6. Prove that for any natural number s the last s digits of the numbers M_n ($n = 1, 2, \dots$) form an infinite periodic sequence, the period being formed of $4 \cdot 5^{s-1}$ terms.

The proof follows from Theorem 1, p. 246, of my paper referred to above.

Many theorems on divisors of numbers M_n have been collected by E. Storchi in paper [1].

2. Theorem of E. Lucas and D. H. Lehmer

THEOREM 3 (¹). *A number M_p, p being an odd prime, is prime if and only if it is a divisor of the $(p-1)$-th term of the sequence $s_1, s_2, \ldots$, where $s_1 = 4$, $s_k = s_{k-1}^2 - 2$, $k = 1, 2, \ldots$*

PROOF. Let $a = 1+\sqrt{3}$, $b = 1-\sqrt{3}$. We have $a+b = 2$, $ab = -2$, $a-b = 2\sqrt{3}$. We define sequences u_n, v_n $(n = 1, 2, \ldots)$ of natural numbers by

$$u_n = \frac{a^n - b^n}{a-b}, \qquad v_n = a^n + b^n.$$

These formulae imply that for any $n = 1, 2, \ldots$ we have

$$u_n = \binom{n}{1} + \binom{n}{3} \cdot 3 + \binom{n}{5} \cdot 3^2 + \ldots, \qquad v_n = 2\left(1 + \binom{n}{2} \cdot 3 + \binom{n}{4} \cdot 3^2 + \ldots\right).$$

Hence for any natural k, l we have

$$(1) \qquad 2u_{k+l} = u_k v_l + v_k u_l,$$

$$(2) \qquad (-2)^{l+1} u_{k-l} = u_l v_k - u_k v_l \quad \text{for} \quad k > l,$$

$$(3) \qquad u_{2k} = u_k v_k,$$

$$(4) \qquad v_{2k} = v_k^2 + (-2)^{k+1},$$

$$(5) \qquad v_k^2 - 12u_k^2 = (-2)^{k+2},$$

$$(6) \qquad 2v_{k+l} = v_k v_l + 12 u_k u_l.$$

For an odd prime q we denote by $\omega(q)$ the least natural number n such that $q \mid u_n$ (provided it exists).

We now prove three following lemmas.

LEMMA 1. *An odd prime q divides u_n, n being a natural number, if and only if $\omega(q) \mid n$.*

PROOF OF LEMMA 1. Let q be a given odd prime number. We denote by S the set of natural numbers n such that $q \mid u_n$. By (1) and (2), if two numbers, k and l, belong to the set S, then number $k+l$ is also a number of the set S, moreover, if $k > l$, then $k-l$ belongs to S. Thus we see that the set S has following property: the sum and the difference (provided it is positive) of

---

(¹) Lehmer [2] (cf. also Kraïtchik [1], p. 141, and Trost [3]).

any two numbers of the set S belong to S. Let d be the least natural number that belongs to S. From the above-mentioned property of the set S, we infer by a simple induction that numbers kd, $k = 1, 2, \ldots$, are in the set S. On the other hand, suppose that a natural number n belongs to S and that n divided by d leaves a positive remainder r. Then $n = td+r$, where t is an integer $\geqslant 0$, and $r < d$. The case $t = 0$ is clearly impossible, since r, being less than d, cannot be equal to n and thus cannot belong to the set S because of the definition of d. Consequently, t is a natural number and thus td belongs to S, whence, by the property of S, number $r = n-td$, as the difference of two numbers of the set S with $n > td$, must belong to S; this, however, contradicts the definition of d. From this we conclude that $r = 0$, which means that the set S is just the set of positive multiples of a number that belongs to it. Therefore if a number n belongs to S, then $\omega(q) \mid n$ and *vice versa*. This proves Lemma 1. ☐

LEMMA 2. *If q is a prime > 3, then*

$$q \mid u_q - 3^{(q-1)/2} \tag{7}$$

and

$$q \mid v_q - 2. \tag{8}$$

PROOF OF LEMMA 2. In order to prove (7) we write

$$u_q = \frac{1}{2\sqrt{3}}[(1+\sqrt{3})^q-(1-\sqrt{3})^q] = \sum_{k=0}^{(q-1)/2} \binom{q}{2k+1} 3^k.$$

In the sum of the right-hand side the binomial coefficients are all divisible by the prime q, except for the last, which is equal to 1; hence formula (7) follows.

In order to prove (8) we write

$$v_q = (1+\sqrt{3})^q+(1-\sqrt{3})^q = 2\sum_{k=0}^{(q-1)/2} \binom{q}{2k} 3^k.$$

In this sum all the binomial coefficients, apart from the first one, are divisible by q; hence formula (8) follows. ☐

LEMMA 3. *If for a prime $q > 3$ the number $\omega(q)$ exists, then $\omega(q) \leqslant q+1$.*

PROOF OF LEMMA 3. Since $u_1 = 1, v_1 = 2$, by (1) and (2) with $k = q, l = 1$, we find $2u_{q+1} = 2u_q+v_q$ and $-4u_{q-1} = 2u_q-v_q$, whence $-8u_{q+1}u_{q-1} = 4u_q^2-v_q^2$. But, in virtue of Lemma 2, we have $q \mid u_q^2-3^{q-1}$ and $q \mid v_q^2-4$.

Since q is a prime > 3, by the theorem of Fermat we obtain $q \mid 3^{q-1}-1$. Therefore we have $q \mid u_q^2-1$ and so $q \mid 4u_q^2-v_q^2$. Consequently $q \mid 8u_{q+1}u_{q-1}$, which, by $q > 3$, implies that either $q \mid u_{q+1}$ or $q \mid u_{q-1}$. In the former case, in virtue of Lemma 1 we obtain $\omega(q) \leqslant q+1$, in the latter we have $\omega(q) \leqslant q-1$. Thus, in any case, $\omega(q) \leqslant q+1$, which shows the validity of Lemma 3. □

We now turn to the proof of sufficiency of the condition of Theorem 3. Suppose that p is an odd prime and let $M_p \mid s_{p-1}$. Then

$$M_p \mid 2^{2^{p-2}} s_{p-1}. \tag{9}$$

We have $2s_1 = v_2$. For a natural number n suppose that $2^{2^{n-1}}s_n = v_{2^n}$, this being true for $n = 1$. Since $s_{n+1} = s_n^2-2$, we then have $2^{2^n}s_{n+1} = (2^{2^{n-1}}s_n)^2 - 2^{2^n+1} = v_{2^n}^2 - 2^{2^n+1}$. But, in virtue of (4) with $k = 2^n$, we have $v_{2^{n+1}} = v_{2^n}^2 - 2^{2^n+1}$. Thus $2^{2^n}s_{n+1} = v_{2^{n+1}}$. The formula $2^{2^{n-1}}s_n = v_{2^n}$ is thus proved by induction. Hence, for $n = p-1$ we have

$$2^{2^{p-1}}s_{p-1} = v_{2^{p-1}}. \tag{10}$$

By (10), from (9) we obtain

$$M_p \mid v_{2^{p-1}}, \tag{11}$$

whence, by (3) with $k = 2^{p-1}$,

$$M_p \mid u_{2^p}. \tag{12}$$

Now let q denote an arbitrary prime divisor of M_p. Since, in view of the fact that p is odd, number $M_p = 2^p-1$ is not divisible by 3, we have $q > 3$. The relation $q \mid M_p$ and formula (12) give $q \mid u_{2^p}$, and consequently, by Lemma 1, we have $\omega(q) \mid 2^p$. On the other hand, $\omega(q)$ does not divide 2^{p-1} because, if it did, we would have, by Lemma 1, $q \mid u_{2^{p-1}}$, whence, by (5) with $k = 2^{p-1}$, q would be a divisor of a power of the number 2 which is impossible since q is a prime > 3. Hence $\omega(q) = 2^p$. In virtue of Lemma 3, we then have $2^p \leqslant q+1$, whence $M_p \leqslant q$, which, in virtue of the relation $q \mid M_p$, proves that $M_p = q$, which means that M_p is a prime.

The sufficiency of the condition of Theorem 3 is thus proved. In order to prove the necessity we prove the following

LEMMA 4. *If p is a prime of the form $12k+7$, then $p \mid 3^{(p-1)/2}+1$.*

PROOF OF LEMMA 4. Let p be a prime of the form $12k+7$, where k is an integer $\geqslant 1$. Then $p > 3$ and, by property I of Legendre's symbol (cf.

Chapter IX, § 1), we find $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. By property V of Legendre's symbol we have $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = -1$, whence $\left(\frac{3}{p}\right) = -1$. Consequently $3^{(p-1)/2} \equiv -1 \pmod p$, whence $p \mid 3^{(p-1)/2}+1$, as asserted. ☐

We now turn to the proof of the necessity of the condition of Theorem 3. Suppose that p is a prime > 2 and that the number $q = M_p$ is also a prime. Since $p > 2$, we have $8 \mid 2^p = q+1$. Hence $q = 8t+7$, where t is an integer $\geqslant 0$. We have $q-1 = 2^p-2 = 2(2^{p-1}-1)$. Since $p-1$ is even, i.e. $p-1 = 2s$, where s is a natural number, we have $2^{p-1}-1 = (3+1)^s - 1 = 3u$, where u is an integer. Hence $3 \mid 2^{p-1}-1 \mid q-1 = 8t+6$, whence $3 \mid t$, i.e. $t = 3k$, where k is an integer. Therefore $q = 8t+7 = 24k+7$.

By (4), with $k = 2^{p-1}$, we have

$$v_{2^p} = v_{2^{p-1}}^2 - 4\cdot 2^{2^{p-1}-1}. \tag{13}$$

But since $q = 24k+7 = 8\cdot 3k+7$, by Theorem 1 we find $q \mid M_{(q-1)/2}$, i.e. $q \mid M_{2^{p-1}-1} = 2^{2^{p-1}-1}-1$, whence, by (13),

$$q \mid v_{2^p} - v_{2^{p-1}}^2 + 4. \tag{14}$$

But, by (6) with $k = q$, $l = 1$, and since $q+1 = 2^p$, we have

$$2v_{2^p} = v_q v_1 + 12 u_q u_1 = 2v_q + 12u_q.$$

Consequently,

$$v_{2^p} = v_q + 6u_q = (v_q-2)+6(u_q+1)-4. \tag{15}$$

Since $q = 24k+7$, we may apply Lemma 4 to number q; so $q \mid 3^{(q-1)/2}+1$, and hence, by (7), $q \mid u_q+1$ and, by (8), $q \mid v_q-2$. Thus, by formula (15), $q \mid v_{2^p}+4$, whence by (14), $q \mid v_{2^{p-1}}^2$. This, in view of (10), $q = M_p$ being odd, shows that $M_p \mid s_{p-1}$, and this completes the proof of the necessity of the condition.

Theorem 3 is thus proved. ☐

It is easy to prove that Theorem 3 is equivalent to the following theorem of Lucas:

THEOREM 3^a. *A number M_p, where p is an odd prime, is a prime if and only if number M_p is a divisor of the $(p-1)$-th term of the sequence $t_1, t_2, \ldots$, where $t_1 = 2$, $t_{k+1} = 2t_k^2-1$ for $k = 1, 2, \ldots$*

The proof of equivalence follows immediately from the fact that the sequence s_k $(k = 1, 2, \ldots)$ turns into the sequence t_k $(k = 1, 2, \ldots)$ if s_k is replaced by $2t_k$. Thus, since M_p is odd, the relations $M_p \mid s_{p-1}$ and $M_p \mid t_{p-1}$ are equivalent.

A proof of Theorem 3ª based on the theory of trigonometric functions of complex variable was given by T. Bang [1].

3. How the greatest of the known prime numbers have been found

Theorem 3 cannot be easily applied in investigation of Mersenne numbers whose indices are greater than, say, ten. The reason is that the terms of the sequence s_k ($k = 1, 2, \ldots$) increase very rapidly with k. By induction, it follows from the definition of the sequence ($s_1 = 4$, $s_k = s_{k-1}^2 - 2$, $k = 2, 3, \ldots$) that $s_k \geqslant 10^{2^{k-2}} + 4$ for any $k = 2, 3, \ldots$ Consequently $s_{10} > 10^{2^8} = 10^{256}$, which shows that the tenth term s_{10} has more than 250 digits. Number s_{100} cannot even be written as a decimal as it has more than 10^{27} digits.

Therefore, in order to apply Theorem 3 while investigating whether a given number M_p (p being a prime > 2) is a prime or not, we proceed as follows.

For any integer t we denote by $\bar{t}$ the remainder left by t divided by M_p. Thus for any integer t we have $M_p \mid t - \bar{t}$. Now we define a sequence r_k ($k = 1, 2, \ldots$) by

$$(16) \qquad r_1 = 4, \qquad r_{k+1} = \overline{r_k^2 - 2} \qquad \text{for} \qquad k = 1, 2, \ldots$$

and we prove by induction that

$$(17) \qquad M_p \mid s_k - r_k \qquad \text{for} \qquad k = 1, 2, \ldots$$

We see that (17) is valid for $k = 1$. Suppose that it is true for a natural number k. Then, *a fortiori*, $M_p \mid s_k^2 - r_k^2$, whence $M_p \mid s_k^2 - 2 - (r_k^2 - 2)$. Since $s_k^2 - 2 = s_{k+1}$, and, in view of $M_p \mid t - \bar{t}$ with $t = r_k^2 - 2$, and by (16), $M_p \mid r_k^2 - 2 - r_{k+1}$, we obtain $M_p \mid s_{k+1} - r_{k+1}$. Formula (17) is thus proved by induction on $k = 1, 2, \ldots$

By (17), formula $M_p \mid s_{p-1}$ is equivalent to the formula $M_p \mid r_{p-1}$. By (16) in order to calculate r_{p-1} one has to calculate $p-2$ squares of the numbers which are the remainders obtained by dividing by M_p, these having clearly no more digits than number M_p, and to calculate the remainders left by these squares minus 2 divided by M_p. The electronic computers that exist nowadays are able to carry out the calculation described above for primes p up to about two hundred thousand.

It has been discovered in this way that number M_{293} is composite since it is not a divisor of the corresponding number r_{293}. We do not know any prime divisor of this number.

A situation similar to the one described above arises for M_{347} (see Brillhart, Lehmer, Selfridge, Tuckerman and Wagstaff [1]).

Until the year 1950 the greatest known prime number was M_{127}, which has 39 digits. It was investigated by E. Lucas in 1876 and in 1914 E. Fauquembergue proved it to be a prime. In January 1952 by the use of electronic computers SWAC the numbers M_{521} and M_{607} were proved to be prime. The former has 157 digits, the latter 183 digits. In the same year, in June, the number M_{1279} was proved to be a prime; it has 376 digits. In October 1952, the same was proved by R. M. Robinson about the numbers M_{2203} and M_{2281}, the former having 664 digits, and the latter 687 digits (¹).

The next Mersenne prime M_{3217} was discovered by H. Riesel in 1957 on the BESK computer, and in 1962 Alexander Hurwitz found the subsequent two M_{4253} and M_{4423}, on IBM7090.

A further computation made by D. B. Gillies on ILLIAC II led to the discovery of Mersenne primes M_{9683}, M_{9941} and M_{11213} in 1964. It was as late as 1971 that B. Tuckerman found the next Mersenne prime M_{19937} using IBM 360/91.

The subsequent primes M_{21701}, M_{23209} were discovered by E. Nickel and C. Noll on CDC Cyber 174 in 1978 and 1979 respectively. In 1979 D. Slowinski, using CRAY 1, discovered M_{44497}, in 1983, M_{86243}, M_{132049} and finally, in 1985, M_{216091}. The latter is the largest known prime and it has 65050 digits.

Thus thirty prime Mersenne numbers M_n are known, namely for $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4219, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 132049, 216091$ (Brillhart, Lehmer, Selfridge, Tuckerman and Wagstaff [1]).

For all $n \leqslant 263$ the factorizations of numbers $2^n - 1$ are known. For example, number M_{101} is the product of two primes, the smaller being 7432339208719 (cf. Brillhart et al. [1]).

There was a conjecture that if a Mersenne number M_n is a prime, then the number M_{M_n} is also a prime. This is true for the first four Mersenne prime numbers, but for the fifth, i.e. $M_{13} = 8191$, the conjecture was disproved by D. J. Wheeler in 1953. The number $M_{M_{13}} = 2^{8191} - 1$ (which has 2466 digits) turned out to be composite (cf. Robinson [1], p.

(¹) More details on these large prime numbers are to be found in papers of H. S. Uhler [2], [3].

844). This fact was shown by an application of the theorem of Lucas and Lehmer; the calculation involved was done by an electronic computer and required 100 hours. None of the prime divisor of this number is known. However, in 1957 it was proved that, though the number M_{17} is a prime, the number $M_{M_{17}}$ is composite. It is divisible by $1768\,(2^{17}-1)+1$. Similarly, though the number M_{19} is prime, the number $M_{M_{19}}$ is composite, divisible by $120\,(2^{19}-1)+1$. In this connection there is another conjecture (still undecided): the sequence $q_0, q_1, q_2, \ldots$, where $q_0 = 2$, $q_{n+1} = 2^{q_n}-1$, $n = 0, 1, 2, \ldots$, contains only prime numbers. This has been verified for q_n with $n \leqslant 4$; the number q_5, however, as it is easy to verify, has more than 10^{37} digits, and so it cannot even be written as a decimal. Moreover, since the prime divisors of the number q_5 are of the form $2kq_4+1 > 2q_4$, the number q_5 has no prime divisors that have less than 39 digits. Therefore, at the present time at least, it is impossible to decide whether the number q_5 is prime or not.

4. Prime divisors of Fermat numbers

The Fermat numbers $F_n = 2^{2^n}+1$ $(n = 0, 1, 2, \ldots)$ may be considered as a particular case of the numbers of the form a^n+1, where a is a natural number > 1. Suppose that a number a^m+1, where m is a natural number > 1, is a prime. If m has an odd divisor $k > 1$, then $n = kl$, whence $a^l+1 \mid (a^l)^k+1 = a^m+1$ and, since $k > 1$, the number a^m+1 is composite. Consequently, if a^m+1, where m is a natural number > 1, is a prime, then number m must be a power of number 2, i.e. $m = 2^n$, where n is a natural number. In particular, if 2^m+1, where m is a natural number, is a prime, then it must be a Fermat number.

Hence it follows that in order that a natural number s be a prime Fermat number, it is necessary and sufficient that s be a prime > 2 and $s-1$ have no odd prime divisors. This indicates a method of finding all the Fermat numbers that are prime. The method is a double application of Eratosthenes' sieve. (Compare an analogous method of finding Mersenne numbers, § 1.)

THEOREM 4. *If a is an even integer, n a natural number and p a prime such that $p \mid a^{2^n}+1$, then $p = 2^{n+1}k+1$, where k is a natural number.*

PROOF. Since $p \mid a^{2^n}+1$, we have $p \mid a^{2^{n+1}}-1$; $p \mid a^{2^n}-1$ is impossible, because, if $p \mid 2$, so $p = 2$, which is a contradicition since $p \mid a^{2^n}+1$ implies $(p, a) = 1$, and a is even. Let δ denote the exponent to which a belongs mod p. Since $p \mid a^{2^{n+1}}-1$, by Theorem 9 of Chapter VI we have $\delta \mid 2^{n+1}$, the relation $\delta \mid 2^n$ being impossible, because $p \mid a^{2^n}-1$ does not hold. From this we infer that $\delta = 2^{n+1}$ and, since by the theorem of Fermat $p \mid a^{p-1}-1$, we obtain $\delta \mid p-1$, that is $2^{n+1} \mid p-1$, whence $p = 2^{n+1}k+1$, where k is a natural number, as was to be proved. □

THEOREM 5. *Any divisor* > 1 *of the number* F_n, *where* n *is an integer* > 1, *is of the form* $2^{n+2}k+1$, *where* k *is a natural number.*

PROOF. As follows from the proof of Theorem 4 (with $a = 2$), if p is a prime and $p \mid F_n$, then number 2 belongs to the exponent 2^{n+1} mod p. On the other hand, Theorem 4 implies that p is of the form $2^{n+1}t+1$, where t is a natural number. Consequently, if $n > 1$, it is of the form $8k+1$, whence, as we learned in § 1, the relation $p \mid M_{(p-1)/2}$, i.e. $p \mid 2^{(p-1)/2}-1$, holds. But, since 2 belongs to the exponent 2^{n+1} mod p, we must have $2^{n+1} \mid (p-1)/2$, and so $2^{n+2} \mid p-1$, whence $p = 2^{n+2}k+1$, where k is a natural number.

Thus we see that any prime divisor of the number $F_n (n > 1)$ is of the form $2^{n+2}k+1$. Moreover, since any divisor > 1 of the number F_n is the product of prime divisors of F_n, then it must also be of the above form (because the product of two numbers of the form $mk+1$ is also of this form). Theorem 5 is thus proved. □

Theorem 5 is used in investigations whether a given Fermat number is prime or not. For example, the prime divisors of the number F_4 are, by Theorem 5, of the form $2^6k+1 = 64k+1$. In order to verify whether the number F_4 is prime one has to divide it by primes of this form which are not greater than $\sqrt{F_4}$, i.e. less than 2^8. The only number which satisfies the above conditions is the number 193; therefore, since $F_4 = 65637$ is not divisible by 193, it is prime.

We now turn to the number F_5. By Theorem 5, any prime divisor of it must be of the form $2^7k+1 = 128k+1$. Substituting $k = 1, 2, 3, 4, 5$ we obtain prime numbers for $k = 2$ and $k = 5$ only They are the numbers 257 and 641, respectively. Dividing the number $F_5 = 2^{32}+1$ by these two numbers, we see that it is divisible by the second of them. Consequently, F_5 is composite. As regards the proof that $641 \mid F_5$, an easy elementary proof which does not involve any explicit dividing is at hand. In fact, we have $641 = 5^4+2^4 \mid 5^4 \cdot 2^{28}+2^{32}$ and $641 = 5 \cdot 2^7+1 \mid 5^2 \times 2^{14}-1 \mid 5^4 \cdot 2^{28}-1$, whence 641 is a divisor of the difference of the numbers $5^4 \cdot 2^{28}+2^{32}$ and $5^4 \cdot 2^{28}-1$, i.e. of the number $2^{32}+1 = F_5$.

We have $F_5 = 641 \cdot 6700417$. Since $\sqrt{6700417} < 2600$ and the prime divisors of 6700417 (as divisors of F_5) are of the form $128k+1$, where $k = 5, 6, \ldots$, we see that in order to verify whether 6700417 is prime or not it is sufficient to divide the number by $128k+1$ with $5 \leqslant k \leqslant 20$. This, however, yields a positive remainder for any such k. Thus we see that 6700417 is a prime. The fact that F_5 is the product of two different primes was discovered by Euler in 1732.

The prime divisors of the number F_6 must be of the form $256k+1$. Here the first prime divisor is obtained for $k = 1071$ and is 274177. Therefore the number F_6 is composite, which was found by Landry in 1880. It can be proved that F_6 is, like F_5, the product of two primes.

The prime divisors of the number F_7 must be of the form $512k+1$. Here the first prime divisor corresponding to $k = 116503103764643$ was found by M. J. Morrison and J. Brillhart in 1975 with the aid of the electronic computer IBM 360/91. The cofactor is also a prime.

Earlier, in 1905, J. C. Morehead proved that F_7 is composite, using Theorem 6, see § 5 below.

The prime divisors of the number F_8 must be of the form $1024k+1$. Here the first prime divisor corresponding to $k = 1208689024954$ was found by R. P. Brent in 1980. Earlier, in 1908, J. C. Morehead and A. E. Western proved that F_8 is composite, using Theorem 6, below. Later, in 1981, Brent and H. C. Williams found that it is the product of two prime factors.

The number F_9 is composite. As was found by Western in 1903 the number $2^{11}k+1$, where $k = 2^5 \cdot 37$, is a prime divisor of F_9.

The number F_{10} was found to be composite by J. L. Selfridge in 1953. With the aid of the electronic computer SWAC he found that $2^{12} \cdot 11131 + 1$ is its prime factor. Another prime factor, $2^{14} \cdot 395937+1$ was found by J. Brillhart in 1962 with the aid of IBM 704.

The same problem for the subsequent two numbers was much easier to solve. In 1899 Cunningham found two prime divisors of the number F_{11}; they are $2^{13} \cdot 39+1$ and $2^{13} \cdot 119+1$. For F_{12} four different prime divisors have been found: the divisor $2^{14} \cdot 7+1$ was found by Pervouchine and Lucas in 1877, the divisors $2^{16} \cdot 397+1$ and $2^{16} \cdot 973+1$ were found by Western in 1903, the divisor $2^{14} \cdot 11613415+1$ was found by Hallyburton and Brillhart in 1975. The number F_{13} was proved to be composite by G. A. Paxson and the number F_{14} by J. L. Selfridge and Alexander Hurwitz, but for the latter no prime factor has been found. For the former J. R. Hallyburton and J. Brillhart have recently found the factor $2^{16}\cdot 41365885+1$. Number F_{15} was established to be composite in 1925 by Kraïtchik. He found that $2^{21}\cdot 579+1$ is its prime divisor.

F_{16} was found to be composite in 1953 by Selfridge. By the use of the electronic computer SWAC he found that $2^{19}\cdot 1575+1$ is its prime factor. The importance of this result lies in the fact that it disproves the conjecture that all the terms of the sequence

$$2+1,\quad 2^2+1,\quad 2^{2^2}+1,\quad 2^{2^{2^2}}+1,\quad 2^{2^{2^{2^2}}}+1,\quad \dots$$

are prime numbers. In fact, the number F_{16} (which has 19729 digits) is the fifth term of the sequence.

The question whether F_{17} is composite or not has been answered quite recently. In 1980 G. B. Gostin verified that it is composite, divisible by $2^{19}\cdot 59251857+1$.

The number F_{18} is composite. In 1903 Western found that $2^{20}\cdot 13+1$ is its prime divisor. Also the number F_{19} is composite. In 1962 Riesel found that $2^{21}\cdot 33629+1$ is its prime divisor.

We do not know whether the numbers F_{20}, F_{22} are prime or not. In 1963 Wrathall found that the number F_{21} is composite, divisible by $2^{23}\cdot 534689+1$. In 1878 Pervouchine found that the number F_{23} is composite, he showed that $2^{25}\cdot 5+1$is its prime divisor. At present 84 composite Fermat numbers are known. They are numbers F_n with $n = 5$, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 23, 25, 26, 27, 29, 30, 32, 36, 38, 39, 42, 52, 55, 58, 62, 63, 66, 71, 73, 75, 77, 81, 91, 93, 99, 117, 125, 144, 147, 150, 201, 205, 207, 215, 226, 228, 250, 255, 267, 268, 275, 284, 287, 298, 316, 329, 334, 398, 416, 452, 544, 556, 637, 692, 744, 931, 1551, 1945, 2023, 2089, 2456, 3310, 4724, 6537, 6835, 9428, 9448, 23471 (Keller [1], [2], [3]).

The greatest known composite Fermat number is F_{23471}. It has a prime divisor $2^{23473}\cdot 5+1$. The number of digits of F_{23471} is greater than 10^{7064}, and so we are not able even to write it down. The situation is similar to that described in the first paragraph of § 3 and the divisibility is established by a similar procedure.

In order to check that the number F_n is divisible by m we proceed as follows. We denote by $\bar{t}$ the remainder left by an integer t divided by m. We define the sequence r_k ($k = 1, 2, \dots$) by the conditions

$$r_1 = 2^2,\qquad r_{k+1} = \overline{r_k^2},\qquad k = 1, 2, \dots$$

It is easily proved by induction that

$$m \mid 2^{2^k} - r_k \qquad \text{for} \qquad k = 1, 2, \dots$$

Consequently, in order to establish whether F_n is divisible by m it is sufficient to find whether r_n+1 is divisible by m.

We are unable to prove that there exist infinitely many composite Fermat numbers, or to prove that there is at least one Fermat number $> F_4$ that is prime. The fact that there are many Fermat numbers $> F_4$ which are known to be composite and that there is no such prime Fermat number, has been a source of the conjecture that all the Fermat numbers $> F_4$ are composite.

By Theorem 5, prime divisors of Fermat numbers are of the form $k \cdot 2^m + 1$, where k, m are natural numbers; it has been investigated, therefore, which numbers of this form are prime.

If $k = 1$, the numbers 2^m+1 are prime if and only if they are Fermat numbers. Consequently, we know only five such numbers, for $m = 1, 2, 4, 8, 16$. The least number of this form about which we do not know whether it is prime is the number $2^{2^{20}}+1$. In consequence of what we have said above, there are only four numbers of the form $2 \cdot 2^m+1$ which are known to be prime. They are for $m = 1, 3, 7, 15$. However, we know 24 primes of the form $3 \cdot 2^m+1$. They are obtained for $m = 1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276, 353, 408, 438, 534, 2208, 2816, 3168, 3189, 3912$. There are only three known prime numbers of the form $4 \cdot 2^m+1$, where $m = 1, 2, \ldots$ They are obtained for $m = 2, 6, 14$. There are 17 known primes of the form $5 \cdot 2^m+1$ (where $m = 1, 2, \ldots$), for $m = 1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947, 3313, 4687, 5947, 13165, 23473$. For any natural number $k < 3061$ we know at least one natural number m such that number $k \cdot 2^m+1$ is prime. (It is known that for $k = 3061$ numbers $k \cdot 2^m+1$ are composite for all $m < 17008$, cf. Robinson [2], Cormack and Williams [1], Baillie, Cormack and Williams [1], Jaeschke [1], and Keller [1]). On the other hand it can be proved that there exist infinitely many natural numbers k such that $k \cdot 2^m+1$ is composite for $m = 1, 2, \ldots$; see Exercise 3, below.

For $n = 39$ and $n = 207$ we have $3 \cdot 2^{n+2}+1 \mid F_n$. For any of the numbers $n = 5, 23, 73, 125, 1945, 23471$, we have $5 \cdot 2^{n+2}+1 \mid F_n$ and also $5 \cdot 2^{n+3}+1 \mid F_n$ for $n = 36$ and 3310. If for a number of the form $k \cdot 2^m+1$ we put $k = m = n$, we obtain a *Cullen number* $C_n = n \cdot 2^n+1$ (cf. Beeger [2]). A. J. C. Cunningham and H. J. Woodall [1] proved that any of the Cullen numbers C_n with $1 < n < 141$ is composite and has a small prime divisor. However, it has been proved that number C_{141} is prime (Robinson [2]).

EXERCISES. **1.** Prove that if m is a natural number $\neq 3$, then number 2^m+1 is not a power of a natural number, the exponent being greater than 1.

PROOF. At first we prove that if m is a natural number $\neq 3$, then number 2^m+1 is not the square of a natural number. In fact, if 2^m+1 were equal to n^2, where n is a natural number, then, clearly, n would be odd and greater than 1; moreover, it would be greater than 3, because $n = 3$ gives $m = 3$, contrary to the assumption. Therefore $2^m = n^2-1 = (n-1)(n+1)$, whence $n-1 = 2^k$, $n+1 = 2^{m-k}$, where k would be a natural number contained between 1 and m, $k < m-k$. Hence $2^{m-k}-2^k = 2$, which, in view of the fact that $k > 1$, is impossible. Now suppose that $m \neq 3$ and $2^m+1 = n^8$, where s is a natural number > 2. Since 2^m+1 is not a square, s must be odd. Consequently, $2^m = n^s-1 = (n-1)(n^{s-1}+n^{s-2}+\ldots+n+1)$, which is impossible because the second factor, being a sum of odd numbers, is an odd number > 1. The proof is thus completed. □

2. Prove that for Fermat numbers $m = 2^{2^n}+1$ $(n = 0, 1, 2, \ldots)$ the relation $m \mid 2^m-2$ holds.

PROOF. For any integer $n \geqslant 0$ we have $n+1 \leqslant 2^n$, whence $2^{n+1} \mid 2^{2^n}$ and consequently $2^{2^{n+1}}-1 \mid 2^{2^{2^n}}-1$, and, since $m = 2^{2^n}+1 \mid 2^{2^{n+1}}-1$, we obtain $m \mid 2^{2^{2^n}}-1$, whence, *a fortiori*, $m \mid 2^m-2$. □

REMARK. Hence it follows that composite Fermat numbers are pseudoprime (Chapter V, § 7).

It can be proved that if for a natural number k number $m = 2^k+1$ satisfies the relation $m \mid 2^m-2$, then m is a Fermat number (Jakóbczyk [1], p. 122, Theorem X).

3. Prove that there exist infinitely many natural numbers k such that for any of them number $k \cdot 2^n+1$ is composite for any natural number n.

PROOF. As we have already learned, numbers F_m are prime for $m = 0, 1, 2, 3, 4$; moreover, number F_5 is the product of two prime numbers, 641 and p, where $p > F_4$. By the Chinese remainder theorem, there exist infinitely many natural numbers k that satisfy the two congruences

$$(18) \qquad k \equiv 1 \pmod{(2^{32}-1)641} \quad \text{and} \quad k \equiv -1 \pmod{p}.$$

We are going to prove that if k is any such number and if in addition, it is greater than p, then all the numbers $k \cdot 2^n+1$, $n = 1, 2, \ldots$, are composite.

At first suppose that $n = 2^s(2t+1)$, where s is one of the numbers 0, 1, 2, 3, 4 and t is an arbitrary integer $\geqslant 0$. In virtue of (18), we have $k \cdot 2^n+1 \equiv 2^{2^s(2t+1)}+1 \pmod{2^{32}-1}$ and. since $F_s \mid 2^{32}-1$ and $F_s \mid 2^{2^s(2t+1)}+1$, we infer that number $k \cdot 2^n+1$ is divisible by F_s at the same time being greater than $p > F_s$, it is composite.

Now let $n = 2^5(2t+1)$, where $t = 0, 1, 2, \ldots$ In virtue of (18), we have $k \cdot 2^n+1 \equiv 2^{2^5(2t+1)}+1 \pmod{641}$ and, since $641 \mid 2^{2^5}+1 \mid 2^{2^5(2t+1)}+1$, we infer that number $k \cdot 2^n+1$ is divisible by 641. But it is greater than 641, and so it is composite.

It remains to consider the case where n is divisible by 2^6, i.e. where $n = 2^6t$ for $t = 1, 2, \ldots$ In virtue of formulae (18), we have $k \cdot 2^n+1 \equiv -2^{2^6t}+1 \pmod{p}$. But $p \mid 2^{2^5}+1 \mid 2^{2^6}-1 \mid 2^{2^6t}-1$, whence we infer that number $k \cdot 2^n+1$ is divisible by p and greater than p, and so it is composite.

We have thus proved that number $k \cdot 2^n+1$ is composite for any $n = 1, 2, \ldots$ (cf. Sierpiński [28] and Aigner [1]). □

4. Find all the primes of the form n^n+1, where n is a natural number, that have no more than 300000 digits.

SOLUTION. There are only three primes that satisfy this condition. They are: $1^1+1 = 2$, $2^2+1 = 5$, $4^4+1 = 257$. In fact, if a number n^n+1, where n is a natural number, is a prime, then, clearly, n cannot have any odd divisor > 1, and so it must be of the form $n = 2^k$, where k is a natural number. But then $n^n+1 = 2^{2^k}+1$, whence we infer that k cannot have any odd divisor > 1, and so $k = 2^s$, where s is an integer $\geqslant 0$. Hence it follows that $n^n+1 = F_{2^s+s}$. Thus, for $s = 0$ we obtain number $F_1 = 5$, for $s = 1$ number $F_3 = 257$, for $s = 2$ and $s = 3$ numbers F_6 and F_{11}, which are composite; for $s = 4$ we obtain the number $F_{20} > 2^{2^{20}} > 2^{10^6}$, but this has more than 300000 digits (Sierpiński [20]).

5. Find all the primes of the form $n^{n^n}+1$ that have not more than 10^{616} digits.

SOLUTION. There are only two such numbers: $1^{1^1}+1 = 2$, $2^{2^2}+1 = 17$. The proof is similar to that used in the preceding exercise. We prove first that if $n > 2$ and number $n^{n^n}+1$ is a prime, then $n = 2^{2^s}$, where s is a natural number. Therefore $n^{n^n}+1 = F_{2^{2^s+s}+s}$. For $s = 1, 2$ we obtain the numbers F_9, F_{66} which are composite, for $s = 3$ we obtain number F_{2053} which has more than 10^{616} digits. It follows that, if it is true that there are no prime numbers of the form $n^{n^n}+1$ with $n > 2$, then there exist infinitely many composite Fermat numbers.

6. Prove that among the numbers $2^{2^n}+3$, $n = 1, 2, \ldots$, there are infinitely many composite ones.

PROOF. We are going to show that all the numbers $2^{2^{2k+1}}+3$, where $k = 1, 2, \ldots$, are composite. In fact, as we know, for natural numbers k we have $2^{2k} = 3l+1$, where l is a natural number. Hence $2^{2^{2k+1}}+3 = 2^{6l+2}+3 = 4(2^3)^{2l}+3 \equiv 4+3 \equiv 0 \pmod 7$. But, since for any natural number k number $2^{2^{2k+1}}+3$ is > 7, it is composite. The problem whether among the numbers $2^{2^n}+3$ there exist infinitely many primes remains open. □

7. Prove that any of the numbers $2^{2^n}+5$, $n = 1, 2, \ldots$, is composite.

The proof follows from the fact that all these numbers are divisible by 3.

5. A necessary and sufficient condition for a Fermat number to be a prime

THEOREM 5. *In order that a Fermat number F_n, where n is a natural number, be a prime, it is necessary and sufficient that $F_n \mid 3^{(F_n-1)/2}+1$.*

PROOF. Let n denote a natural number. Suppose that $F_n \mid 3^{(F_n-1)/2}+1$. Then F_n cannot be divisible by 3. Let p be any prime divisor of F_n different from 3. Let δ be the exponent to which 3 belongs mod p. Since $p \mid 3^{F_n-1}-1$, we must have $\delta \mid F_n-1 = 2^{2^n}$. If δ were $< 2^{2^n}$, then $\delta = 2^k$, where k is a non-negative integer $< 2^n$. Consequently, $2^k \mid 2^{2^n-1} = (F_n-1)/2$, so $\delta \mid (F_n-1)/2$ and therefore, since $p \mid 3^\delta-1$, $p \mid 3^{(F_n-1)/2}-1$ and so, by $p \mid F_n$, we would have $p \mid 3^{(F_n-1)/2}+1$, whence $p \mid 2$, so $p = 2$, which is impossible because $p \mid F_n$ and F_n is odd. Therefore $\delta = 2^{2^n}$. But, as we know, $\delta \mid p-1$, whence $p = 2^{2^n}k+1$, where k is a natural number, whence $p \geqslant 2^{2^n}+1 = F_n$ and, since $p \mid F_n$, we see that $F_n = p$, which proves that F_n is a prime. The condition is thus proved to be sufficient.

In order to show that the condition is necessary we prove the following

LEMMA. *If p is a prime of the form $12k+5$, then $p \mid 3^{(p-1)/2}+1$.*

PROOF OF THE LEMMA. If p is a prime and $p = 12k+5$, then, by the properties of Legendre's symbol, $\left(\dfrac{p}{3}\right) = \left(\dfrac{-1}{3}\right) = -1$, whence, by property V of Legendre's symbol, $\left(\dfrac{3}{p}\right)\left(\dfrac{p}{3}\right) = 1$. Consequently $\left(\dfrac{3}{p}\right) = -1$, and so $3^{(p-1)/2} \equiv -1 \pmod{p}$, which gives $p \mid 3^{(p-1)/2}+1$, as required. □

Now let n be a natural number. The number $F_n = 2^{2^n}+1$ is of the form $12k+5$ because for any natural number n we have $2^n = 2m$, and, as it is easy to verify (by simple induction for example) that $4^m \equiv 4 \pmod{12}$ for any $m = 1, 2, \ldots$ Consequently $F_n = 4^m+1 \equiv 5 \pmod{12}$, i.e. $F_n = 12k+5$ and, if F_n is a prime, then, by the lemma, $F_n \mid 3^{(F_n-1)/2}+1$.

Thus we see that the condition of Theorem 5 is sufficient. □

Theorem 5 is thus proved. It implies that if F_n is a prime, then number 3 is a primitive root of the number F_n. (The proof is obtained simply by noting that the number 3 belongs to the exponent F_n-1 mod F_n, which actually follows from the proof of Theorem 5).

The useful procedure for applying Theorem 5 in order to decide whether a Fermat number F_n is prime or not is as follows. We denote by t the remainder left by F_n divided by an integer t and set

$$r_1 = 3, \qquad r_{k+1} = \overline{r_k^2}, \qquad k = 1, 2, \ldots$$

By an easy induction we verify that $F_n \mid 3^{2^{k-1}}-r_k$ holds for any $k = 1, 2, \ldots$. Hence, for $k = 2^n$, we find $F_n \mid 3^{(F_n-1)/2}-r_{2^n}$. From this we infer that number $3^{(F_n-1)/2}+1$ is congruent to $r_{2^n}+1$ mod F_n.

This is the very method by which the numbers F_7, F_8, F_{13} and F_{14} have been proved to be composite.

The number F_7 has 39 digits, so in order to find the number $r_{2^7}+1 = r_{128}+1$, necessary for applying the procedure described above, some hundred and thirty squares of natural numbers, each having less than 39 digits, had to be calculated. Moreover, each of these squares had to be divided by the number F_7 (which has 39 digits). Nowadays the calculation described above is not difficult to perform owing to the use of electronic computers, but in the year 1905, i.e. when Morehead obtained this result, the task was very tedious, although it could be performed.

A similar method was applied to F_8, F_{13} and F_{14} in order to find that they are also composite numbers. The method described above gives no information about the prime divisors of the number under consideration; neither it gives any decomposition of the number into a product of two factors greater than 1. This is why we do not know any such decomposition of the number F_{14}.

The next Fermat number, whose character is unknown, namely F_{20}, has more that 300000 digits; the calculations involved in the procedure described above, and used to show that numbers F_7, F_8, F_{13} and F_{14} are composite involve in this case over a milion divisions of numbers that have well over hundred thousand digits, each by a number that has over 300000 digits.

EXERCISE. Find the least prime divisor of number $12^{2^{15}}+1$.

SOLUTION. By Theorem 4, each prime divisor p of number $12^{2^{15}}+1$ is of the form $2^{16}k+1$, where k is a natural number. Consequently, $p \geqslant 2^{16}+1 = F_4$. Since F_4 is a prime, by Theorem 5 we have $F_4 \mid 3^{2^{15}}+1$. Hence $3^{2^{15}} \equiv -1 \pmod{F_4}$. But, in virtue of the theorem of Fermat, $2^{2^{16}} = 2^{F_4-1} \equiv 1 \pmod{F_4}$, whence $4^{2^{15}} \equiv 1 \pmod{F_4}$. Therefore $12^{2^{15}} = 3^{2^{15}} \cdot 4^{2^{15}} \equiv -1 \pmod{F_4}$, so $F_4 \mid 12^{2^{15}}+1$. Thus we see that number F_4 is the least prime divisor of number $12^{2^{15}}+1$, the latter being $> F_4$ and thus composite. We do not know whether there are infinitely many composite numbers among the numbers $12^{2^n}+1$, where $n = 1, 2, \ldots$, or whether there are infinitely many primes among them.

CHAPTER XI

REPRESENTATIONS OF NATURAL NUMBERS AS SUMS OF NON-NEGATIVE *k*th POWERS

1. Sums of two squares

THEOREM 1. *A natural number n is the sum of two squares of integers if and only if the factorization of n into prime factors does not contain any prime of the form* $4k+3$ *that has an odd exponent.*

LEMMA. *If an odd prime p divides the sum of the squares of two relatively prime integers, then it must be of the form* $4k+1$.

PROOF OF THE LEMMA. Let a, b be two relatively prime integers and p an odd prime such that $p \mid a^2+b^2$. Then $a^2 \equiv -b^2 \pmod{p}$; this, raised to the $(p-1)/2$-th power gives $a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} \pmod{p}$. But, since $(a, b) = 1$, the numbers a, b are not divisible by p, whence, by the theorem of Fermat, $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$; consequently, $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$, which by $p > 2$, gives $(-1)^{(p-1)/2} = 1$ and proves that $(p-1)/2$ is even. Therefore p must be of the form $4k+1$. ☐

PROOF OF THE THEOREM. Suppose that a number n can be represented as the sum of the squares of two integers,

$$n = a^2+b^2. \tag{1}$$

Let

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s} \tag{2}$$

be the factorization of n into prime factors. Finally, let p be a prime divisor of the form $4k+3$ of the number n. Write $d = (a, b)$, $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$. In virtue of (1), $d^2 \mid n$, and so $n = d^2 n_1$, where n_1 is a natural number. Suppose that the exponent of p in factorization (2) is odd. Then, since $n = d^2 n_1$, we must have $p \mid n_1 = a_1^2+b_1^2$, which contradicts the lemma. Thus we have proved that the condition of the theorem is necessary.

In order to prove that it is sufficient we note that without any loss of generality we may assume that n is greater than 1, since for the number 1 we have $1 = 1^2+0^2$. Suppose that (2) is the factorization of n into prime factors. Let m be the greatest natural number whose squares divides n. Then $n = m^2k$, where k either is equal to 1 or is a product of different prime numbers among which no prime of the form $4k+3$ occurs. Since $2 = 1^2+1^2$, in virtue of Theorem 9 of Chapter V, each of these primes is the sum of the squares of two natural numbers. The identity

$$(a^2+b^2)(c^2+d^2) = (ab+cd)^2+(ad-bc)^2$$

represents the product of two (and, by induction, of any finite number) natural numbers, each of them being the sum of the squares of two integers, as the sum of the squares of two integers. Consequently, k is the sum of the squares of two integers. So $k = u^2+v^2$, whence $n = m^2k = (mu)^2+(mv)^2$. This completes the proof of sufficiency of the condition. Theorem 1 is thus proved. □

In connection with Theorem 1 the question arises how many different representations as sums of two squares a natural number n admits. The answer to this question is to be found in Chapter XIII, § 9.

COROLLARY. *If a natural number is not the sum of the squares of two integers, then it is not the sum of the squares of two rational numbers either.*

PROOF. If a natural number n is not the sum of the squares of two integers, then, by Theorem 1, there is a prime p of the form $4k+3$ that divides n to an odd power exactly. Suppose that $n = \left(\frac{l}{m}\right)^2+\left(\frac{l_1}{m_1}\right)^2$ where m, m_1 are natural numbers and l, l_1 are integers. Then $(mm_1)^2n = (lm_1)^2+(l_1 m)^2$. But p must appear with an odd exponent in the factorization of the left-hand side of the equality and, by Theorem 1, this cannot be true regarding the right-hand side of the equality; thus a contradiction is reached and so the corollary is proved. □

As proved by E. Landau [1], if $f(x)$ denotes the number of natural numbers $\leqslant x$ that are sums of two squares, then $f(x)\colon \frac{x}{\sqrt{\log x}}$ tends to a finite positive limit as x increases to infinity.

The representations $n = x^2+y^2$, where x, y are integers, $0 \leqslant x \leqslant y$, and $n \leqslant 10000$, are given by A. van Wijngarden [1]. The number of decompositions of n into two squares for $n \leqslant 20000$ is given by H. Gupta [2]. For primes $p \leqslant 10007401$ of the form $4k+1$ the tables of such decompositions have been given by Kogbetlianz and Krikorian [1].

EXERCISES. **1.** Find a necessary and sufficient condition for a rational number l/m to be the sum of the squares of two rational numbers.

SOLUTION. Such a condition is that the number lm be the sum of the squares of two integers. We easily verify it on the basis of the remark that, if $\frac{l}{m} = \left(\frac{l_1}{m_1}\right)^2 + \left(\frac{l_2}{m_2}\right)^2$, then $lm(m_1 m_2)^2 = (mm_2 l_1)^2 + (mm_1 l_2)^2$. On the other hand, if $lm = a^2+b^2$, then $\frac{l}{m} = \left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2$.

REMARK. Exercise 1 and Theorem 1 imply that an irreducible fraction l/m, where l, m are natural numbers, is the sum of the squares of two rational numbers if and only if each of the numbers l, m is the sum of the squares of two integers.

2. Prove that if a rational $r \neq 0$ is the sum of the squares of two rationals, then it has infinitely many representations as the sum of the squares of two positive rationals.

PROOF. First, we suppose that $r = a^2+b^2$, where a, b are rationals both different from zero. Therefore, without loss of generality, we may assume that a, b are positive and that $a \geqslant b$. For any natural k we have

$$r = \left(\frac{(k^2-1)a-2kb}{k^2+1}\right)^2 + \left(\frac{(k^2-1)b+2ka}{k^2+1}\right)^2,$$

which gives a representation of r as the sum of the squares of two rationals. If $k \geqslant 3$, we have $3k^2-8k = 3k(k-3)+k \geqslant 3$, whence

$$\frac{k^2-1}{2k} \geqslant \frac{4}{3} > \frac{b}{a} \quad \text{and so} \quad a_k = \frac{(k^2-1)a-2kb}{k^2+1} > 0.$$

Moreover it is easy to prove that a_k increases with k. Therefore numbers a_k are all different and, for $k \geqslant 3$, positive. This, for $k \geqslant 3$, gives different representations of r as sums of the squares of positive rationals. Thus we see that r admits infinitely many such representations.

Now we suppose that $r = a^2$, where a is a rational. Since $r \neq 0$, we may assume that $a > 0$. For natural k we have

$$r = \left(\frac{(k^2-1)a}{k^2+1}\right)^2 + \left(\frac{2ka}{k^2+1}\right)^2$$

As it is easy to prove, numbers $a_k = (k^2-1)a/(k^2+1)$ increase with k. Consequently, there are infinitely many representations of the number r into sums of the squares of positive rational numbers. □

3. Given a natural number m, find a natural number n that has at least m different representations as the sum of the squares of two natural numbers.

SOLUTION. Let $n = a^2$, where $a = (3^2+1)(4^2+1)\dots((m+2)^2+1)$. The numbers $a/(k^2+1)$ are natural for any $k = 3, 4, \dots, m+2$. Consequently also the numbers

$$a_k = \frac{k^2-1}{k^2+1}a, \quad b_k = \frac{2ka}{k^2+1} \qquad (k = 3, 4, \dots, m+2)$$

are natural. But, in virtue of the identity

$$a^2 = \left(\frac{k^2-1}{k^2+1}a\right)^2 + \left(\frac{2ka}{k^2+1}\right)^2,$$

if $a_k = \dfrac{k^2-1}{k^2+1}a$, $b_k = \dfrac{2ka}{k^2+1}$, we have $n = a^2 = a_k^2+b_k^2$, $k = 3, 4, \dots, m+2$. But

$$a_k - b_k = \frac{k^2-2k-1}{k^2+1}a = \frac{(k-1)^2-2}{k^2+1}a > 0 \quad \text{for} \quad k = 3, 4, \dots, m+2$$

and

$$a_k = a - \frac{2a}{k^2+1}, \quad \text{whence} \quad a_3 < a_4 < \dots < a_{m+2}.$$

Thus we see that the representations $n = a_k^2+b_k^2$, $k = 3, 4, \dots, m+2$, are all different, their number being m. Therefore the number n has the required properties.

At the same time we have proved that for a given natural number m there exist at least m non-congruent Pythagorean triangles that have the same hypothenuse.

4. Given: a representation as the sum of two squares of a natural number n. Find a similar representation of the number $2n$.

SOLUTION. If $n = a^2+b^2$, then $2n = (a+b)^2+(a-b)^2$.

2. The average number of representations as sums of two squares

Now our aim is to consider the problem how to find all the representations of a given natural number as sums of two squares.

If n is representable as the sum of two squares, i.e. if

$$n = x^2+y^2, \tag{3}$$

then $n \geqslant x^2$ and $n \geqslant y^2$, whence $|x| \leqslant \sqrt{n}$, $|y| \leqslant \sqrt{n}$. Thus, to solve the problem, it is sufficient to substitute for x in (3) integers whose absolute values are not greater than $\sqrt{n}$ each, and see whether the number $n-x^2$ is a square or not. If $n-x^2$ is a square, then, putting $y = \pm\sqrt{n-x^2}$, we obtain a representation of n as the sum of two squares. If $n-x^2$ is not a square, such a representation is not obtained. It is plain that we may confine our consideration to non-negative x's only because the change of the sign of x does not cause any change of the value of $n-x^2$. It is worthwhile to notice that the sequence n, $n-1^2$, $n-2^2$, $n-3^2, \dots$ has the following property: the differences of the consecutive numbers of the sequence are 1, 3, 5, ..., i.e. they form the sequence of odd natural numbers.

EXAMPLES. Let $n = 10$. We form the sequence 10, 9, 6, 1. In this sequence the second term and the fourth term are squares so we put $x = \pm 1$, $y = \pm 3$ or $x = \pm 3$, $y = \pm 1$. Thus eight decompositions are obtained. They are

$$\begin{aligned}10 &= 1^2+3^2 = 1^2+(-3)^2 = (-1)^2+3^2 = (-1)^2+(-3)^2 = 3^2+1^2\\ &= 3^2+(-1)^2 = (-3)^2+1^2 = (-3)^2+(-1)^2.\end{aligned}$$

Now let $n = 25$. We form the sequence 25, 24, 21, 16, 9, 0. Here 25, 16, 9, 0 are squares. Therefore for x, y the following values are obtained:

$$x = 0,\quad y = \pm 5;\qquad x = \pm 3,\quad y = \pm 4;\qquad x = \pm 4,\quad y = \pm 3;$$
$$x = \pm 5,\quad y = 0$$

(where all combinations of the signs $\pm$ are allowed). Thus 25 has 12 representations as sums of two squares.

Let $\tau(n)$ denote the number of all the representations of a natural number n as sums of two squares, two representations being regarded as different also when they differ in the order of summands only. As above, we find

$$\begin{array}{lllll}\tau(1) = 4, & \tau(2) = 4, & \tau(3) = 0, & \tau(4) = 4, & \tau(5) = 8,\\ \tau(6) = 0, & \tau(7) = 0, & \tau(8) = 4, & \tau(9) = 4, & \tau(10) = 8.\end{array}$$

As we have proved in § 5, Chapter V, each prime of the form $4k+1$ has a unique representation (apart from the order of the summands) as the sum of two squares. This shows that for any prime p of the form $4k+1$ we have $\tau(p) = 8$. The reasoning presented above shows that for any natural number n the inequality $\tau(n) \leqslant 4\sqrt{n}$ holds. Exercise 3 of § 1 implies that there is no upper bound for $\tau(n)$.

Now we are going to calculate the sum

$$T(n) = \tau(1)+\tau(2)+ \ldots +\tau(n). \tag{4}$$

The number $\tau(k)$ is the number of solutions of the equation $x^2+y^2 = k$ in integers x, y. Hence the number $T(n)$ is the number of solutions of the inequalities

$$0 < x^2+y^2 \leqslant n. \tag{5}$$

We divide the solutions of (5) into classes by saying that two solutions belong to the same class if and only if the values of x are equal. We are going to find the number of solutions in each of these classes.

If $x = 0$, then, by (5), y may assume integral values such that $y^2 \leqslant n$, i.e. $|y| \leqslant \sqrt{n}$. As it is easy to verify, the number of such y's is $2[\sqrt{n}]$. If $x = k \neq 0$, then, by (5), we must have $k^2 \leqslant n$; so $|k| \leqslant \sqrt{n}$ and $y^2 \leqslant n-k^2$, whence $|y| \leqslant \sqrt{n-k^2}$. The number of those y's is $1+2[\sqrt{n-k^2}]$ (number 1 must be added since $y = 0$ is included). Since k may assume any of the values $\pm 1, \pm 2, \ldots, \pm[\sqrt{n}]$ and the sign $\pm$ has no influence on the value of k^2, we obtain

$$2[\sqrt{n}]+2\sum_{k=1}^{[\sqrt{n}]}(1+2[\sqrt{n-k^2}]) = 4[\sqrt{n}]+4\sum_{k=1}^{[\sqrt{n}]}[\sqrt{n-k^2}]$$

and so

$$T(n) = 4\sum_{k=0}^{[\sqrt{n}]}[\sqrt{n-k^2}]. \tag{6}$$

Thus, for example, for $n = 100$ we have

$$\begin{aligned}T(100) = 4([\sqrt{100}]+[\sqrt{99}]+[\sqrt{96}]+[\sqrt{91}]+[\sqrt{84}]+[\sqrt{75}]+\\ +[\sqrt{64}]+[\sqrt{51}]+[\sqrt{36}]+[\sqrt{19}]) = 4(10+9+9+9+9+8+\\ +8+7+6+4) = 316.\end{aligned}$$

Sum (4) has a simple geometric interpretation. Since, as we have learned, number $1+T(n)$ is the number of pairs of integers that satisfy the inequality $x^2+y^2 \leqslant n$, it is equal to the number of points of the plane whose coordinates are integers (these being called *lattice* points) inside or on the circumference of a circle C whose centre is placed at the point $(0, 0)$ and radius is equal to $\sqrt{n}$. To cut it short, number $1+T(n)$ is equal to the number of lattice points that are inside or on the circumference of circle C.

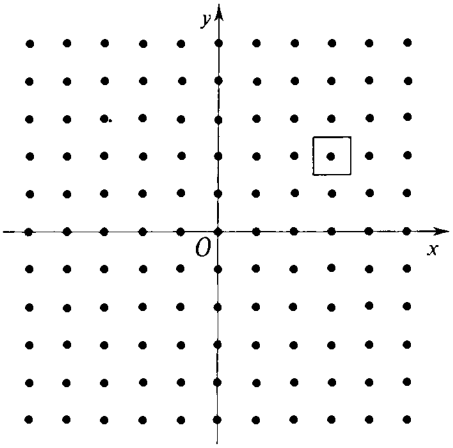

Fig. 1

Now, to each lattice point we assign a square in which the middle point is a lattice point, the sides are parallel to the axes of coordinates and the area is equal to 1 (see Fig. 1). The area P covered by the squares assigned to the lattice points that are not outside the circle C is equal to the number of these points, and so it is equal to $1+T(n)$. The circle C_1

the centre of which is $(0, 0)$ and radius $\sqrt{n}+\frac{1}{\sqrt{2}}$ contains (inside and on the circumference) all the points covered by the squares assigned to the points of the circle C. This is evident, since $1/\sqrt{2}$ is the greatest possible distance from a point of a square of area 1 to its middle points. Therefore the area P is less than the area of the circle C_1. Hence $P \leqslant \pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2$. On the other hand, the area of the circle C_2, whose centre is also $(0, 0)$ and radius is $\sqrt{n}-\frac{1}{\sqrt{2}}$, is less than P, so $P > \pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2$. This, by the equality $P = 1+T(n)$, gives

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2-1 < T(n) < \pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2-1. \tag{7}$$

We note that $\pi\sqrt{2} < 5$ and that, for any natural number n, $0 < \frac{1}{2}\pi-1 < 1 \leqslant \sqrt{n}$. Hence

$$\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2-1 = \pi n+\pi\sqrt{2}\sqrt{n}+\tfrac{1}{2}\pi-1 < \pi n+6\sqrt{n},$$

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2-1 = \pi n-\pi\sqrt{2}\sqrt{n}+\tfrac{1}{2}\pi-1 > \pi n-6\sqrt{n}.$$

From this, by (7), we obtain $\pi n-6\sqrt{n} < T(n) < \pi n+6\sqrt{n}$, whence $T(n)-\pi n| < 6\sqrt{n}$ for any natural number n, whence

$$\left|\frac{T(n)}{n}-\pi\right| < \frac{6}{\sqrt{n}}. \tag{8}$$

From (8) and (4) it follows that

$$\lim_{n\to\infty}\frac{\tau(1)+\tau(2)+\ldots+\tau(n)}{n} = \pi,$$

which means that the mean value of the function $\tau(n)$ is π. This can also be expressed by saying that on the average there are π representations of a natural number as the sum of two squares. As we have found above, $T(100) = 316$ (i.e. natural numbers not greater than 100 have, on the average, 3.16 decompositions into the sum of two squares); similarly, by

(6), we can easily find that $T(400) = 1256$, whence $T(400)/400 = 3.14$, and $T(1000) = 3148$, whence $T(1000)/1000 = 3.148$.

By formula (6), $T(n)$ can be calculated for any n (though the calculation may be very long), this, by (8), indicates a method of calculating the number π with a given accuracy.

In virtue of (8), we have $|T(n)-\pi n| < 6\sqrt{n}$ for any natural number n. In the year 1906, I used the method of Voronoï to find that there exist a constant A such that $|T(n)-\pi n| < A\sqrt[3]{n}$ (Sierpiński [1]). After that, stronger results were obtained by van der Corput and others; for the best result at present, see Ivić [1].

As so far we have calculated the number of lattice points that are contained in a circle whose centre is (0, 0), which, of course, is a lattice point. In 1957, H. Steinhaus [1] proposed the following exercise: *prove that for any natural number n there exists such a circle on the plane that contains precisely n lattice points.*

We are going to show that if $p = (\sqrt{2}, \frac{1}{3})$, then for any natural number n there is a circle C_n with centre p containing precisely n lattice points inside.

Suppose that two different lattice points (x_1, y_1) and (x_2, y_2) are at equal distances from the point p. Then

$$(x_1-\sqrt{2})^2+(y_1-\tfrac{1}{3})^2 = (x_2-\sqrt{2})^2+(y_2-\tfrac{1}{3})^2.$$

Hence

$$2(x_2-x_1)\sqrt{2} = x_2^2+y_2^2-x_1^2-y_1^2+\tfrac{2}{3}(y_1-y_2).$$

Since $\sqrt{2}$ is irrational, $x_1-x_2 = 0$, whence $y_2^2-y_1^2+\frac{2}{3}(y_1-y_2) = 0$, and so $(y_2-y_1)(y_2+y_1-\frac{2}{3}) = 0$. But $y_2+y_1-\frac{2}{3} \neq 0$ because y_1 and y_2 are integers, consequently $y_2-y_1 = 0$. This gives $x_1 = x_2$ and $y_1 = y_2$, contrary to the assumption that the points are different.

Now let n denote an arbitrary natural number. It is clear that any circle C with centre p and a radius large enough contains more than n lattice points. It is also clear that the number of lattice points contained in C is finite. Since, in virtue of what we proved above, the distances from p to the lattice points are all different, we may arrange the lattice points that are inside circle C in the sequence $p_1, p_2, \ldots, p_n, p_{n+1}, \ldots$ according to their distances from the point p. Let C_n denote the circle whose centre is p and radius is equal to the distance of the point p_{n+1} from the point p. It is plain that the only lattice points inside circle C_n are the points $p_1, p_2, \ldots, p_n$.

Consequently, circle C_n possesses the required properties; the theorem of Steinhaus is thus proved.

It is not difficult to prove that there is no point p in the plane whose coordinates are rationals such that for any natural number n there exists a circle with centre p which contains precisely n lattice points (cf. Sierpiński [19], p. 26).

On the other hand, it can be proved that for any natural n there exists a circle whose centre has rational coordinates and which contains precisely n lattice points inside.

Let us mention here that H. Steinhaus has proved that for any natural number n there exists a circle with area n containing precisely n lattice points inside. However, the proof of this statement is difficult.

It can be proved that for any natural number n there exists a square that contains precisely n lattice points inside (cf. Sierpiński [19], pp. 28–30).

It is also true that for any natural number n in the three-dimensional space there exists a sphere that contains precisely n points whose coordinates are integers.

In order to prove this it is sufficient to note firstly that if u, v, w are rational numbers such that $u\sqrt{2}+v\sqrt{3}+w\sqrt{5}$ is a rational, then $u = v = w = 0$, and secondly that any sphere whose centre is at the point $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and radius is equal to 3 contains at least one point whose coordinates are all integers. From these two facts the proof is deduced as in the case of the circle in the plane.

J. Browkin has proved, that for any natural number n there exists a cube (in the three-dimensional space) that contains inside precisely n points whose coordinates are integers.

A. Schinzel [7] has proved that *for any natural number n there exists a circle on the circumference of which there are precisely n lattice points*. As a matter of fact, what he has proved is that if n is odd, i.e. $n = 2k+1$, where k is a non-negative integer, then the circle with centre $(\frac{1}{3}, 0)$ and radius $5^k/3$ has the required property. If n is even, i.e. if $n = 2k$, where k is a natural number, then the circle with centre $(\frac{1}{2}, 0)$ and radius $5^{(k-1)/2}/2$ has the required property.

T. Kulikowski [1] has proved that for any natural number n there exists a sphere (in the three-dimensional space), on the boundary of which there are precisely n points whose coordinates are integers. He generalized this theorem for sphères in spaces of an arbitrary $\geqslant 3$ dimension.

Rational points (i.e. points whose coordinates are rational numbers) on the circumference of a circle have also been investigated. There exist circles in the plane in which there are no rational points; for example, such is the circle $x^2+y^2 = 3$. There are circles on which there lies precisely one rational point, for example, on the circle $(x-\sqrt{2})^2+(y-\sqrt{2})^2 = 4$ there is precisely one rational point, namely the point (0, 0). There are also circles on which there are precisely two rational points, for example, such is the circle $x^2+(y-\sqrt{2})^2 = 3$, the only rational points on it being (1, 0) and (−1, 0).

In general, we prove that *if there are three rational points on a circle, then there are infinitely many rational points on it.* It is easy to prove that if there are three rational points on a circle, then the centre of the circle is a rational point and the square of the radius of the circle is also rational. Since by subtracting a rational number from two rational numbers successively we again obtain rational numbers, then, without any loss of generality, we may assume that the centre of the circle is the point (0, 0). Denote this circle by C. It is not difficult to prove that if C contains at least one rational point, then it must contain infinitely many rational points. In fact, if a, b are rationals such that $a^2+b^2 = r^2$, then for any rational number t the point (x, y) where $x = \dfrac{2at+b(1-t^2)}{1+t^2}$, $y = \dfrac{a(1-t^2)-2bt}{1+t^2}$ is rational and $x^2+y^2 = r^2$.

We sum up the facts thus obtained in saying that for a given circle only the following cases are possible: it contains no rational points, it contains precisely one rational point, it contains precisely two rational points, or finally, it contains infinitely many rational points. It can be proved that, in the last case, rational points form a dense subset of the circle, which means that on any arc of the circle there is a rational point.

It has been proved (cf. Sierpiński [21]) that if r^2 is a rational number, then the circle C with radius r contains infinitely many points such that the distance of any two of them is a rational number. As an immediate consequence of this we infer that for any natural number n there exists a circle which contains n points such that the distance of any two of them is a natural number. This again has an important consequence, namely that for any natural n there exists a set consisting of n points no three of which lie on one line such that the distance of any two of them is a natural number. This theorem was first proved by N. H. Anning and P. Erdös (their proof was different) (¹). The authors proved also that if in an infinite set of points in the plane the distance of any two points of the set is integral, then all the points lie on a straight line (cf. Erdös [6] and Trost [2]).

EXERCISE. Prove that the set of rational points of the plane can be divided into two subsets, one having finitely many points in common with any vertical line, the other having finitely many points in common with any horizontal line.

PROOF. As is easy to see, the condition will be satisfied if the first subset consists of the points $\left(\frac{l}{m}, \frac{r}{s}\right)$, the fractions being irreducible and such that the numerators are integral and the denominators natural, and that they satisfy the relation $|l|+m < |r|+s$. The second subset comprises all the rest of the rational points of the plane.

It can be proved that the set of points in the three-dimensional space whose coordinates are rational can be divided into three parts such that each part has finite interesection with any line parallel to a coordinate line (fixed for the part). The same statement for the set of all points of the three-dimensional space is equivalent to the continuum hypothesis (cf. Sierpiński [13] and [22], p. 397). ☐

3. Sums of two squares of natural numbers

THEOREM 2. *A natural number n is the sum of the squares of two natural numbers if and only if all prime factors of the form* $4k+3$ *of the number n have even exponents in the standard factorization of n into primes and either the prime* 2 *has an odd exponent (in the factorization of n) or n has at least one prime divisor of the form* $4k+1$.

PROOF. Suppose that there exists a natural number which is the sum of the squares of two natural numbers, and has the following properties: it does not possess a prime divisor of the form $4k+1$, and in its factorization into primes the prime 2 has even exponent $\geqslant 0$. Let n be the least natural number with these properties. Since it is the sum of the squares of two natural numbers, by Theorem 1 all prime factors of n of the form $4k+3$ have even exponents in the standard form of n. Consequently, $n = 2^{2k}m^2$, where m is an odd natural number and k is an integer $\geqslant 0$. Thus we may write $2^{2k}m^2 = a^2+b^2$, where a, b are natural numbers. If $k > 0$, then the left-hand side of the last equality is divisible by 4; consequently the numbers a, b are both even, i.e. $a = 2a_1$, $b = 2b_1$,

---

(¹) Anning and Erdös [1]; see also Hadwiger [1], p. 85, where a list of references is given.

whence $2^{2(k-1)}m^2 = a_1^2+b_1^2 < n$, contrary to the definition of n. Hence $k = 0$ and so $n = m^2 = a^2+b^2 > 1$. The numbers a, b must be relatively prime because in the case $(a, b) = d > 1$ we would have $a = da_2$, $b = db_2$, where a_2, b_2 are natural numbers, whence $m = dm_1$ and $m_1^2 = a_2^2+b_2^2 < m^2 = n$, contrary to the definition of n. So $(a, b) = 1$. But, since m is odd and > 1 (having no prime divisor of the form $4k+1$), it has a prime divisor $p = 4k+3$. This implies that $p \mid a^2+b^2$, whence $a^2 \equiv -b^2 \pmod{p}$. If we raise each side of the last congruence to the $(2k+1)$th power, then, by the fact that $2(2k+1) = p-1$ and by the theorem of Fermat, we obtain $1 \equiv (-1)^{2k+1} \pmod{p}$, which is impossible.

We have thus proved that a natural number that is the sum of the squares of two natural numbers has the following property: either in its factorization into prime factors the prime 2 has an odd exponent, or it has a prime divisor of the form $4k+1$. Moreover, by Theorem 1, it follows that all prime divisors of the form $4k+3$ have even exponents in the factorization of the number into primes. This shows that the condition of Theorem 2 is necessary.

Now, suppose that a natural number n satisfies the conditions of the theorem. Thus we have either $n = 2m^2$ or $n = 2^\alpha m^2 l$, where $\alpha = 0$ or 1 and l is the product of prime factors of the form $4k+1$. If $n = 2m^2$, then $n = m^2+m^2$, and so it is the sum of the squares of two natural numbers. Suppose that $n = 2^\alpha m^2 l$, where l is the product of primes of the form $4k+1$. By Theorem 9, Chapter V, each of the factors is the sum of two positive squares. But the product of two odd numbers, each of them the sum of two positive squares, is again the sum of two positive squares. The argument to this is that, if $n_1 = a^2+b^2$, $n_2 = c^2+d^2$, where n_1, n_2 are odd, then one of the numbers a and b, say a, must be odd, the other being even; the same is true for the numbers c, d; so let c be odd, d even. Then $n_1 n_2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2+(ac-bd)^2$, where $ac-bd$ is odd, and so $\neq 0$. Thus we see that the number $n_1 n_2$ is the sum of the squares of two natural numbers. By induction, we infer that the same remains true for an arbitrary number of factors of the form $4k+1$. Hence we conclude that the number l is the sum of the squares of two natural numbers, i.e. $l = a^2+b^2$, whence $m^2 l = (ma)^2+(mb)^2$ and $2m^2 l = (ma+mb)^2+(ma-mb)^2$ and $ma-mb \neq 0$ (because a must be different from b since the number $l = a^2+b^2$ is odd). Thus we see that in any event the number n is the sum of the squares of two natural numbers. Therefore the condition of Theorem 2 is sufficient.

Theorem 2 is thus proved. ☐

From Theorem 2 it follows that in order that a square n^2 be the sum of two squares of two natural numbers it is necessary and sufficient that the number n should have at least one prime divisor of the form $4k+1$. This can be expressed by saying that

A natural number n is a hypotenuse of a Pythagorean triangle if and only if n has at least one prime divisor of the form $4k+1$.

Cf. also the corollary to Exercise 3, § 1.

EXERCISES. 1. Prove that a natural number n is the sum of the squares of two different natural numbers if and only if (i) the primes of the form $4k+3$ which appear in the factorization of n into prime factors have even exponents, (ii) the number n has at least one prime divisor of the form $4k+1$.

PROOF. The necessity of condition (i) follows from Theorem 1. Suppose that a natural number n does not satisfy condition (ii), i.e. that it has no prime divisor of the form $4k+1$. Consequently, if $n = a^2+b^2$ for two different natural numbers a, b, then, for $d = (a, b)$, we have $n = d^2(a_1^2+b_1^2)$, where $a = da_1$, $b = db_1$ and a_1, b_1 are different relatively prime natural numbers. Number $a_1^2+b_1^2$ has no prime divisor of the form $4k+1$, and so, since $(a_1, b_1) = 1$, the reasoning used in the proof of Theorem 2 shows that number $a_1^2+b_1^2$ has no prime divisor of the form $4k+3$, either. Therefore $a_1^2+b_1^2 = 2^s$, where s is a natural number > 1, since a_1, b_1 are different natural numbers. Consequently, number $a_1^2+b_1^2$ is divisible by 4, whence it follows that the numbers a_1, b_1 are even, but this contradicts the fact that $(a_1, b_1) = 1$.

Now suppose that a natural number n satisfies conditions (i) and (ii). Then, by Theorem 2, we have $n = a^2+b^2$, where a, b are natural numbers. If $a = b$, then $n = 2a^2$ and, since n satisfies condition (ii), it has a prime divisor of the form $4k+1$, so, in virtue of what we have shown above, a is the hypotenuse of a Pythagorean triangle. This means that $a^2 = c^2+d^2$, where c, d are natural numbers. Clearly $c \neq d$ since, if $c = d$, then $a^2 = 2c^2$, which, in view of the fact that $\sqrt{2}$ is irrational, is impossible. Hence $n = 2a^2 = (c+d)^2+(c-d)^2$, where $c-d \neq 0$ and $c+d \neq c-d$ (since d is a natural number). Consequently, n is the sum of the squares of two different natural numbers. Thus we see that conditions (i) and (ii) are sufficient. This completes the proof. ☐

2. Prove that a natural number n is the sum of the squares of two relatively prime natural numbers if and only if n is divisible neither by 4 nor by a natural number of the form $4k+3$.

PROOF. Suppose that a natural number n is the sum of the squares of two relatively prime natural numbers: $n = a^2+b^2$. If $n = 4k$, then the numbers a, b are both even, contrary to $(a, b) = 1$. If n has a divisor of the form $4k+3$, then, as we know, it has a prime divisor of this form, which, as was shown in the proof of Theorem 2, cannot divide the sum of the squares of two relatively prime natural numbers. Thus we see that the condition is necessary. Suppose that a natural number n satisfies the condition. If $n = 2$, then $n = 1^2+1^2$, and so it is the sum of the squares of two relatively prime natural numbers. If $n > 2$, then the condition implies that n is the product of prime numbers of the form $4k+1$ or the product of number 2 and primes of the form $4k+1$. In the former case n is odd and each of the prime factors of n is the sum of the squares of two relatively prime natural numbers. Hence, by

Lemma 2 and by Exercise 8 of § 5, Chapter V, simple induction shows that n is the sum of the squares of two relatively prime natural numbers. In the latter case, i.e. if n is the product of number 2 and the primes of the form $4k+1$, we have $n = 2(a^2+b^2)$, where a, b are two relatively prime natural numbers. Since a^2+b^2 is odd, one of the numbers a, b is odd and the other is even. We have $n = (a+b)^2+(a-b)^2$, where $a+b$ and $a-b$ are odd natural numbers; moreover, they are relatively prime because if $d \mid a+b$ and $d \mid a-b$, where d is a natural number, then $d \mid 2a$ and $d \mid 2b$; since d, as a divisor of an odd number $a+b$, is odd, we have $d \mid a$ and $d \mid b$, which, in virtue of $(a, b) = 1$, implies $d = 1$. Therefore $(a+b, a-b) = 1$. We have thus proved that the condition is sufficient and the proof is completed. ☐

4. Sums of three squares

THEOREM 3. *A natural number n can be the sum of three squares only if it is not of the form $4^l(8k+7)$, where k, l are integers $\geqslant 0$.*

PROOF. Suppose that there exist natural numbers of the form $4^l(8k+7)$, where k, l are integers $\geqslant 0$, that are the sums of the squares of three integers. Let n be the least of them. We then have $n = 4^l(8k+7) = a^2+b^2+c^2$, where a, b, c are integers. If among the numbers a, b, c there is precisely one odd number, then the sum of their squares is of the form $4t+1$, and so it is different from n. If two of the numbers a, b, c are odd, then the sum of their squares is of the form $4t+2$, and so it is $\neq n$. If all the numbers a, b, c are odd, then the sum of their squares is of the form $8t+3$, and so it is $\neq n$, Consequently, each of the numbers a, b, c must be even. We put $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, where a_1, b_1, c_1 are integers. Hence $4^{l-1}(8k+7) = a_1^2+b_1^2+c_1^2$, contrary to the definition of n. Thus we have proved that no natural number of the form $4^l(8k+7)$, where k, l are non-negative integers, can be the sum of the squares of three integers, and this is precisely what Theorem 3 asserts. ☐

It can be shown that the condition of Theorem 3 is also sufficient in order that a number n be the sum of the squares of three integers. Gauss was the first to prove that *every natural number which is not of the form $4^l(8k+7)$, k and l being non-negative integers, is the sum of the squares of three integers.*

The original proof of Gauss was simplified by Lejeune Dirichlet and Landau (cf. Landau [2], vol. I, pp. 114–125). More recently N. C. Ankeny [1] gave an "elementary" proof of the theorem of Gauss. His proof is based on the theorem of Minkowski concerning lattice points contained in a convex body and on the theorem on arithmetical progression (cf. Mordell [7], Wójcik [1]).

As an immediate consequence of the theorem of Gauss we infer that every natural number of the form $8k+3$ is the sum of the squares of three integers, which, of course, must all be odd. Thus

$$8k+3 = (2a+1)^2+(2b+1)^2+(2c+1)^2,$$

where a, b, c are non-negative integers. Hence

$$k = \frac{a(a+1)}{2}+\frac{b(b+1)}{2}+\frac{c(c+1)}{2} = t_a+t_b+t_c.$$

Thus the theorem of Gauss implies a theorem (first formulated by Fermat) stating that *any natural number is the sum of three or fewer triangular numbers.*

As regards numbers of the form $8k+1$, it follows from the work of B. Jones and G. Pall [1] that except 1 and 25 all of them are sums of the squares of three natural numbers. Among the numbers of the form $8k+5$ that are less than $5\cdot 10^{10}$ only the numbers 5, 13, 37 and 85 are not sums of the squares of three natural numbers. No number of the form $8k+7$ is the sum of the squares of three integers, and so, *a fortiori*, it cannot be the sum of the squares of three natural numbers. A number of the form $4k$ is the sum of the squares of three natural numbers if and only if k itself is the sum of three such squares. In fact, if $4k = a^2+b^2+c^2$, where a, b, c are natural numbers, then, as is easy to see, the numbers a, b, c must be even, and so $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, where a_1, b_1, c_1 are natural numbers. Hence $k = a_1^2+b_1^2+c_1^2$. Conversely, the last equality implies that $4k = (2a_1)^2+(2b_1)^2+(2c_1)^2$. From this we easily deduce that no number of the form 2^n, $n = 1, 2, \ldots$ is the sum of three positive squares. But $8\cdot 3n^2 = (2n)^2+(2n)^2+(4n)^2$, and so we see that among the numbers of the form $8k$ there exist infinitely many natural numbers which are sums of the squares of three natural numbers and infinitely many numbers which are not sums of three squares. As regards the numbers $8k+2$, G. Pall [1] says: "It is conjectured that every $2(8n+1)$ except 2 is a sum of three positive squares". As noticed by A. Schinzel [1] this conjecture is false: the number $2(8\cdot 8+1) = 130$ is not the sum of the squares of three natural numbers (cf. Exercise 1, below).

There is no other exception below $5\cdot 10^{10}$, while among the numbers $2(8n+5)$ there are two, namely 10 and 58.

A number of the form $8k+4$ is the sum of the squares of three natural numbers if and only if number $2k+1$ has this property. Consequently, numbers $8(4k+3)+4 = 4(8k+7)$, $k = 0, 1, 2, \ldots$ are not sums of the squares of three natural numbers. On the other hand, numbers $8(4k+1)$

$+4 = 4(8k+3)$, $k = 0, 1, 2, \ldots$ are sums of the squares of three natural numbers. Any number of the form $8k+6$ is the sum of the squares of three natural numbers because, as follows from the theorem of Gauss, it is the sum of the squares of three integers; it cannot, however, be the sum of two squares because $8k+6 = 2(4k+3)$.

It follows from the results on *numeri idonei* quoted in § 6 of Chapter V via the theory of quadratic forms that at most one number of the form $8k+2$ or $8k+5$ greater than 130 is not the sum of the squares of three natural numbers (see Grosswald, Calloway and Calloway [1], and Schinzel [10]).

Denote by $\tau_3(n)$ the number of different representations of a number n as the sum of the squares of three integers. For $n \leqslant 10$ we have $\tau_3(1) = 6$, $\tau_3(2) = 12$, $\tau_3(3) = 8$, $\tau_3(4) = 6$, $\tau_3(5) = 24$, $\tau_3(6) = 24$, $\tau_3(7) = 0$, $\tau_3(8) = 12$, $\tau_3(9) = 30$, $\tau_3(10) = 24$.

Theorem 3 implies that for infinitely many n's we have $\tau_3(n) = 0$.

As regards the number $T_3(n) = \tau_3(1)+\tau_3(2)+ \ldots +\tau_3(n)$, a geometric argument, similar to that used in § 2 for the sum of two squares (we replace rational points of the plane by points of the three-dimensional space, whose coordinates are integers and we consider spheres and cubes instead of circles and squares, respectively), gives the inequality

$$\frac{4}{3}\pi\left(\sqrt{n}-\frac{\sqrt{3}}{2}\right)^3 - 1 < T_3(n) < \frac{4}{3}\pi\left(\sqrt{n}+\frac{\sqrt{3}}{2}\right)^3 - 1.$$

From this we obtain for all natural numbers n the evaluation

$$|T_3(n) - \tfrac{4}{3}\pi n\sqrt{n}| < 10n,$$

whence it follows

$$\lim_{n\to\infty}\frac{T_3(n)}{\frac{4}{3}\pi n\sqrt{n}} = 1.$$

Denote by $f(x)$ the number of natural numbers x which are representable as sums of three squares. From Gauss's theorem it follows that the number $x - f(x)$ is precisely the number of numbers $\leqslant x$ which are of the form $4^l(8k+7)$, where k, l are integers $\geqslant 0$. Therefore, for a given non-negative integer l we have $8(k+1)-1 \leqslant 4^{-l}x$, and so $k+1 \leqslant \frac{1}{8}(4^{-l}x+1)$, the number of k's $\geqslant 0$ being clearly $\left[\frac{1}{8}(4^{-l}x+1)\right]$. Hence, as an immediate consequence, we obtain

$$x - f(x) = \sum_{l=0}^{[x]}\left[\frac{4^{-l}x+1}{8}\right].$$

If $l > \log x/\log 4$, then $4^l > x > x/7$, whence $(4^{-l}x+1)/8 < 1$. Consequently

$$x-f(x) = \sum_{l=0}^{[\log x/\log 4]} \left[\frac{4^{-l}x+1}{8}\right],$$

and so

$$x-f(x) = \sum_{l=0}^{[\log x/\log 4]} \frac{4^{-l}x+1}{8} - a\left(\frac{\log x}{\log 4}+1\right), \quad \text{where} \quad 0 \leqslant a < 1.$$

But

$$\sum_{l=[\log x/\log 4]+1}^{\infty} 4^{-l} = \frac{4}{3}\cdot 4^{-[\log x \log 4]-1} < \frac{4}{3}\cdot 4^{-\log x/\log 4} = \frac{4}{3x}.$$

Since $\sum_{l=0}^{\infty} \frac{4^{-l}x}{8} = \frac{x}{6}$, we obtain $\lim_{x\to+\infty} \frac{x-f(x)}{x} = \frac{1}{6}$, whence

$$\lim_{x\to+\infty} \frac{f(x)}{x} = \frac{5}{6}.$$

This formula was discovered by Landau in 1908. Let us mention here that M. C. Chakrabarti [1] has investigated the function

$$g(x) = \frac{f(x)-\frac{5}{6}x}{\log x}$$

and has proved that $\liminf_{x\to+\infty} g(x) = 0$, $\limsup_{x\to+\infty} g(x) = \frac{1}{\log 8}$ and that the values of the function $g(x)$ are dense in the interval $\left(0, \frac{1}{\log 8}\right)$.

EXERCISES. **1.** Prove that 130 is not representable as the sum of three positive squares.

PROOF. Suppose that $130 = a^2+b^2+c^2$, where a, b, c are natural numbers. Without loss of generality we may assume that $a \geqslant b \geqslant c$. Consequently, $a^2+1+1 \leqslant 130 \leqslant 3a^2$, whence $43 < a^2 \leqslant 128$, and so $7 \leqslant a \leqslant 11$. But $130-7^2 = 81 = 3^4$, $130-8^2 = 66 = 2\cdot 3\cdot 11$, $130-9^2 = 49 = 7^2$, $130-10^2 = 30 = 2\cdot 3\cdot 5$, $130-11^2 = 9 = 3^2$; thus, looking at the factorizations of numbers 81, 66, 49, 30, 9 into primes, we see that none of them satisfies the condition of Theorem 2, and so none of them is the sum of the squares of two natural numbers. Thus the assumption that 130 is the sum of the squares of three natural numbers leads to a contradiction. □

REMARK. It is easy to prove that 130 is the least natural number of the form $2(8k+1)$ which is not the sum of the squares of three natural numbers.

2. Using the theorem of Gauss prove that a natural number is the sum of the squares of three rational numbers if and only if it is the sum of the squares of three integers.

PROOF. Suppose that a natural number n is the sum of the squares of three rational numbers. Reducing all the three rational numbers to the same denominator, we may write $m^2n = a^2+b^2+c^2$, where a, b, c are integers. If $n = 4^l(8k+7)$, where k, l are integers $\geqslant 0$, then, putting $m = 2^r(2s+1)$, s and r being non-negative integers, we obtain $m^2n = 4^{k+r}(8t+7)$, where $k+r$ and t are non-negative integers. But, in virtue of Theorem 3, this is impossible because $m^2n = a^2+b^2+c^2$. Consequently, number n cannot be of the form $4^l(8k+7)$, where k, l are integers. Thus, by the theorem of Gauss, it is the sum of the squares of three integers. Thus we see that the condition is necessary; plainly it is sufficient as well. ☐

3. Prove that there are no rational numbers x, y, z that satisfy the equation $x^2+y^2+z^2+x+y+z = 1$.

PROOF. The equation is equivalent to the equation

$$(2x+1)^2+(2y+1)^2+(2z+1)^2 = 7. \tag{9}$$

In the proof of Exercise 2 we proved (without using Gauss's theorem) that no number of the form $4^l(8k+7)$, where k and l are non-negative integers, can be the sum of the squares of three rationals. Thus, in particular, number 7 cannot be such a sum, which, in turn, implies that numbers x, y, z cannot satisfy equation (9). ☐

4. Making use of the theorem of Gauss prove that any odd natural number is of the form $a^2+b^2+2c^2$, where a, b, c are integers.

PROOF. Let t be an arbitrary non-negative integer. Number $4t+2$ is not of the form $4^l(8k+7)$, where k, l are non-negative integers. Therefore, by Gauss's theorem, $4t+2 = x^2+y^2+z^2$, where x, y, z are integers. Not all of them are even, since the left-hand side of the equality is not divisible by 4. However, the number of odd numbers among them must be even (since the left-hand side is even); therefore let x, y be odd, z being even, i.e. $z = 2c$. The numbers $x+y$ and $x-y$ are even, and so $x+y = 2a$, $x-y = 2b$, whence $x = a+b$, $y = a-b$. Hence $4t+2 = (a+b)^2+(a-b)^2+4c^2$, whence $2t+1 = a^2+b^2+2c^2$, where a, b, c are integers. This completes the proof. ☐

5. Deduce from the theorem of Gauss that any natural number is either of the form $a^2+b^2+c^2$ or of the form $a^2+b^2+2c^2$, where a, b, c are integers.

PROOF. If a natural number is not a sum of three squares, then, by Gauss's theorem, it is of the form $4^l(8k+7)$, where k, l are non-negative integers. But, by Exercise 4, $8k+7 = x^2+y^2+2z^2$, where $x, y\ z$ are integers. Hence $4^l(8k+7) = (2^lx)^2+(2^ly)^2+2(2^lz)^2$, and so our number is of the form $a^2+b^2+2c^2$, where a, b, c are integers. ☐

6. Prove that if a number $\neq 0$ is representable as the sum of the squares of three rationals, then it has infinitely many representations in this form.

PROOF. This theorem is an immediate consequence of the theorem proved in Exercise 2 of § 1 which says that a number $\neq 0$ which is representable as the sum of the squares of two rationals has infinitely many representations in this form. ☐

7. Prove that the theorem of E. Lionnet stating that each odd natural number is the sum of the squares of four integers two of which are consecutive numbers is a consequence of the theorem of Gauss.

PROOF. Let $n = 2k+1$, where $k = 0, 1, 2, \ldots$ From the theorem of Gauss it follows that the number $4k+1$ is the sum of three squares; consequently $4k+1 = x^2+y^2+z^2$. As it is easy to notice, one of the numbers x, y, z must be odd, the other being even. Let $x = 2a, y = 2b, z = 2c+1$, where a, b, c are integers. Hence $n = 2k+1 = (a+b)^2+(a-b)^2+c^2+(c+1)^2$, which was to be proved. □

8. Show that there exist infinitely many primes of the form $a^2+b^2+c^2+1$, where a, b, c are natural numbers. For the proof use Gauss's theorem.

PROOF. By Theorem 1, Chapter IX, there exist infinitely many primes of the form $8k+7$. If p is a prime of this form, then $p-1 = 8k+6$. But, as we have already learned, Gauss's theorem implies that any number of the form $8k+6$ is the sum of the squares of three natural numbers. Thus $p-1 = a^2+b^2+c^2$, where a, b, c are natural numbers, and so $p = a^2+b^2+c^2+1$. □

9. Find an example showing that the product of two numbers, each of them the sum of three squares, need not be a sum of three squares.

SOLUTION. $63 = 3\cdot 21 = (1^2+1^2+1^2)(1^2+2^2+4^2)$. The number 63, however, being of the form $8k+7$, cannot be the sum of three squares.

10. Deduce from the theorem of Gauss that every natural number is representable as the sum of ten (or fewer) squares of odd numbers (¹).

PROOF. As we know, Gauss's theorem implies that every natural number of the form $8k+3$, where k is an integer $\geqslant 0$, is the sum of the squares of three odd numbers. On the other hand, any natural number $n \geqslant 3$ is of the form $8k+3+r$, where $r = 0, 1, 2, 3, 4, 5, 6, 7$. We see that r is the sum of at most seven squares of the number 1, consequently, n is the sum of the squares of at most 10 squares of odd natural numbers. There exist infinitely many natural numbers that are not representable as sums of fewer than 10 squares of odd natural numbers (cf. Exercise 12, below). □

REMARK. The theorem, which we have just proved, and which we shall call for the time being Theorem T, implies that every natural number of the form $8k+3$, where k is a non-negative integer, is the sum of the squares of three odd numbers.

In fact, by theorem T, if $k \geqslant 0$, then

$$(*)\qquad 8k+3 = n_1^2+n_2^2+\ldots+n_s^2,$$

where s is a natural number $\leqslant 10$, $n_1, n_2, \ldots, n_s$ being odd. Thus we have $n_i^2 \equiv 1 \pmod 8$ for $i = 1, 2, \ldots, s$ and so, by $(*)$, $3 \equiv s \pmod 8$, which in virtue of the inequality $1 \leqslant s \leqslant 10$, proves that $s = 3$. Therefore, by $(*)$, the number $8k+3$ is the sum of the squares of three odd numbers (cf. Sierpiński [8]).

11. Prove that the sth power, s being a natural number, of the sum of the squares of three integers, is also the sum of three squares.

PROOF. If s is 1 or 2, the proof is immediate. Therefore it is sufficient to consider the case where s is of the form $2k+3$, k being a non-negative integer. We have $n^{2k+3} = (n^k)^2n^3$, therefore it is sufficient to prove our theorem for $s = 3$. But this follows immediately from the identity of Catalan:

$$(x^2+y^2+z^2)^3 = x^2(3z^2-x^2-y^2)^2+y^2(3z^2-x^2-y^2)^2+z^2(z^2-3x^2-3y^2)^2. \quad \square$$

(¹) This theorem has been stated without proof by F. Pollock [1], and has been proved by S. Turski [1].

12. Prove that there exist infinitely many natural numbers that are not representable as sums of fewer than ten squares of odd natural numbers.

PROOF. Such are numbers of the form $72k+42$, where $k = 0, 1, 2, \ldots$ In fact, suppose that a natural number $n = 72k+42$ is the sum of the squares of $s < 10$ odd natural numbers. Since the square of an odd natural number is $\equiv 1 \pmod 8$, we have $n \equiv s \pmod 8$, whence, since $n = 72t+42 \equiv 2 \pmod 8$, we have $s \equiv 2 \pmod 8$. But this, by the fact that $0 < s < 10$, gives $s = 2$. Consequently, n is the sum of two squares. But this is impossible because $n = 3(24t+14) = 9(8t+4)+6$ is divisible by 3 but not divisible by 9. Similarly, we can prove that none of the numbers $72k+66$, $k = 0, 1, 2, \ldots$, is the sum of fewer than ten squares. □

5. Representation by four squares

We are going to prove the following theorem known as Lagrange's theorem.

THEOREM 4 (Lagrange). *Every non-negative integer is representable as a sum of four squares.*

LEMMA 1. *Suppose that an odd prime p is a divisor of the sum of the squares of four integers, at least one of which is not divisible by p. Then p is the sum of four squares.*

PROOF OF LEMMA 1. Suppose that a prime p satisfies the assumption of the lemma. Then there is a multiple of p which is the sum of the squares of four integers not all of which are divisible by p. Let n be the least such multiple of p. We then have

$$n = mp, \tag{10}$$

where m is a natural number, and

$$n = a^2+b^2+c^2+d^2, \tag{11}$$

where a, b, c, d are integers, of which at least one, say a, is not divisible by p. Let a_0, b_0, c_0, d_0 be integers such that

$$a_0 \equiv a \pmod p, \quad b_0 \equiv b \pmod p, \quad c_0 \equiv c \pmod p, \quad d_0 \equiv d \pmod p \tag{12}$$

and

$$|a_0| < p/2, \quad |b_0| < p/2, \quad |c_0| < p/2, \quad |d_0| < p/2 \tag{13}$$

(in order to find the number a_0, for instance, it suffices to find the remainder r left by a divided by p and to put $a_0 = r$ if $r < p/2$, or $a_0 = r-p$ if $r > p/2$).

Since a is not divisible by p, so is a_0 and, by a successive application of (12), (10) and (11), we have

$$a_0^2+b_0^2+c_0^2+d_0^2 \equiv a^2+b^2+c^2+d^2 \equiv 0 \pmod{p}.$$

Hence, by the definition of n, in view of (13), we infer

$$n \leqslant a_0^2+b_0^2+c_0^2+d_0^2 < 4(p/2)^2.$$

Consequently, $n < p^2$, which, by (10), implies $mp < p^2$, whence

(14) $$m < p.$$

In virtue of (10) and (11), it remains to prove that $m = 1$. Suppose that $m \neq 1$. Since m is a natural number, by (14) we have

(15) $$1 < m < p.$$

We find natural numbers a_1, b_1, c_1, d_1 that satisfy the conditions

(16) $$a_1 \equiv a \pmod{m}, \quad b_1 \equiv b \pmod{m}, \quad c_1 \equiv c \pmod{m}; \quad d_1 \equiv d \pmod{m}$$

and

(17) $$|a_1| \leqslant m/2, \quad |b_1| \leqslant m/2, \quad |c_1| \leqslant m/2, \quad |d_1| \leqslant m/2.$$

By (16) we see that $a_1^2+b_1^2+c_1^2+d_1^2 \equiv a^2+b^2+c^2+d^2 \pmod{m}$, whence by (11) and (10), we obtain $m \mid a_1^2+b_1^2+c_1^2+d_1^2$, so

(18) $$a_1^2+b_1^2+c_1^2+d_1^2 = ml,$$

where l is an integer $\geqslant 0$.

If $l = 0$, then by (18), $a_1 = b_1 = c_1 = d_1 = 0$, whence, by (16) all the numbers a, b, c, d are divisible by m, whence, by (11), n is divisible by m^2 and so, by (10), $m \mid p$, contrary to (15), since p is a prime. Consequently, l is a natural number.

Suppose that

(19) $$|a_1| = |b_1| = |c_1| = |d_1| = m/2,$$

this being possible only in the case of even m, i.e. when

(20) $$m = 2k,$$

where k is a natural number. The congruence $a_1 \equiv a \pmod{m}$ gives $a = a_1+mt$, where t is an integer. Therefore, by (20) and (19) we have $a = \pm k+2kt = (2t\pm 1)k = k_1 k$, where k_1 is odd. Similarly we find

$$a = k_1 k, \quad b = k_2 k, \quad c = k_3 k, \quad d = k_4 k,$$

where k_1, k_2, k_3, k_4 are all odd numbers. Hence, by (20), (10) and (11) we obtain $n = 2kp = k^2(k_1^2+k_2^2+k_3^2+k_4^2)$. Consequently, $2p = k(k_1^2+k_2^2+k_3^2+k_4^2)$. The square of an odd number is congruent to $1 \pmod 4$, whence we infer that the second factor of the right-hand side of the last equality is divisible by 4, and so $2 \mid p$, contrary to the assumption. This shows that equalities (19) cannot hold. Consequently, for at least one of the inequalities of (17) the equality is impossible. This implies that $a_1^2+b_1^2+c_1^2+d_1^2 < 4 \cdot \dfrac{m^2}{4}$, whence by (18), we obtain $ml < m^2$, so

$$l < m. \tag{21}$$

Consider the identity of Euler

$$\begin{aligned}(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2) &= (aa_1+bb_1+cc_1+dd_1)^2+\\ &+(ab_1-ba_1+cd_1-dc_1)^2+(ac_1-ca_1+db_1-bd_1)^2+\\ &+(ad_1-da_1+bc_1-cb_1)^2.\end{aligned} \tag{22}$$

Its left-hand side, is, by (11), (10) and (18), equal to m^2lp.

By (16) we have

$$\begin{gathered}a_1 = a+ma_2, \quad b_1 = b+mb_2, \quad c_1 = c+mc_2,\\ d_1 = d+md_2,\end{gathered} \tag{23}$$

where a_2, b_2, c_2, d_2 are integers. By (11) and (10), formulae (23) give

$$\begin{aligned}aa_1+bb_1+cc_1+dd_1 &= a^2+b^2+c^2+d^2+m(aa_2+bb_2+cc_2+dd_2)\\ &= m(p+aa_2+bb_2+cc_2+dd_2) = mt_1,\\ ab_1-ba_1+cd_1-dc_1 &= m(ab_2-ba_2+cd_2-dc_2) = mt_2,\\ ac_1-ca_1+db_1-bd_1 &= m(ac_2-ca_2+db_2-bd_2) = mt_3,\\ ad_1-da_1+bc_1-cb_1 &= m(ad_2-da_2+bc_2-cb_2) = mt_4,\end{aligned}$$

where t_1, t_2, t_3, t_4 are integers. Substituting them in the right-hand side of (22), the left-hand side of which is m^2lp, we obtain $m^2lp = m^2(t_1^2+t_2^2+t_3^2+t_4^2)$, whence

$$lp = t_1^2+t_2^2+t_3^2+t_4^2. \tag{24}$$

If the numbers t_1, t_2, t_3, t_4 were all divisible by p, then $p^2 \mid lp$, and so $p \mid l$, which is impossible, since l is a natural number and, by (21) and (14), $l < p$. Formula (24) gives a representation of the number lp as the sum of the squares of four integers, not all of which are divisible by p. It follows from the definition of n that $n \leqslant lp$, and so, by (10), $mp \leqslant lp$, whence $m \leqslant l$, contrary to (21). Thus we see that the assumption that $m \neq 1$ leads to a contradiction; consequently m must be equal to 1, and this is precisely what was to be proved. □

LEMMA 2. *Every prime number is the sum of four squares.*

PROOF OF LEMMA 2. We have $2 = 1^2+1^2+0^2+0^2$, therefore there is no loss of generality in assuming that p is an odd prime. By Lemma 1 it is sufficient to show that p is a divisor of the sum of the squares of four integers which are not all divisible by p. The remainders obtained by dividing the numbers

$$1+0^2, 1+1^2, \ldots, 1+\left(\frac{p-1}{2}\right)^2 \tag{25}$$

by p are different because, as we have already learned (cf. Chapter V, § 5), the numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ divided by p leave different remainders. Similarly, the numbers

$$-0^2, -1^2, \ldots, -\left(\frac{p-1}{2}\right)^2 \tag{26}$$

divided by p leave different remainders. Suppose that the remainders obtained by dividing the numbers of (25) by p are all different from the remainders obtained by dividing the numbers of (26) by p. Then the total number of different remainders obtained by dividing both the numbers of (25) and those of (26) would be equal to $2\left(1+\frac{p-1}{2}\right) = p+1$, which is impossible. Consequently, there exists at least one term of sequence (25), say $1+x^2$, that leaves the same remainder as a term, say $-y^2$, of sequence (26). We have $p \mid 1^2+x^2+y^2+0^2$, which shows that p is a divisor of the sum of the squares of four integers one of which (here the number 1) is not divisible by p. Hence, by Lemma 1, p is the sum of the squares of four integers. The proof of Lemma 2 is thus completed. ☐

PROOF OF THEOREM 4. In virtue of identity (22), the product of two numbers, each of them the sum of four squares, is also the sum of four squares. This, by induction, extends to any finite number of factors. Hence, since any number > 1 is a product of primes, we infer by Lemma 2 that the number itself is the sum of four squares. Since, moreover, $0 = 0^2+0^2+0^2+0^2$ and $1 = 1^2+0^2+0^2+0^2$, the theorem is proved. ☐

Let us mention here a result of D. H. Lehmer [4] saying that among natural numbers only the numbers 1, 2, 5, 7, 11, 15, 23 and the numbers of the form $4^h m$, where $h = 0, 1, 2, \ldots, m = 2$, 6, or 14, are such that the representation of any of them as the sum of four squares is unique apart from the order of the summands.

S. Ramanujan [2] has investigated the systems of natural numbers a, b, c, d such that any natural number n is representable in the form $ax^2+by^2+cz^2+dt^2$, where x, y, z, t are integers. He has proved that for a fixed order of a, b, c, d, say for $a \leqslant b \leqslant c \leqslant d$, there are only 54 such systems, namely $1, 1, 1, d$, where $d = 1, 2, \ldots, 7$; $1, 1, 2, d$, where $d = 2, 3, \ldots, 14$; $1, 1, 3, d$ where $d = 3, 4, 5, 6$; $1, 2, 2, d$, where $d = 2, 3, \ldots, 7$; $1, 2, 3, d$, where $d = 3, 4, \ldots, 10$; $1, 2, 4, d$, where $d = 4, 5, \ldots, 14$; $1, 2, 5, d$, where $d = 6, 7, \ldots, 10$ (cf. Dickson [6], p. 104, Theorem 95).

We now prove the following theorem of Jacobi:

Any natural number is of the form $x^2+2y^2+3z^2+6t^2$, where x, y, z, t are integers.

PROOF. Let n be a natural number. By Theorem 4 there exist integers a, b, c, d such that

$$n = a^2+b^2+c^2+d^2. \tag{27}$$

We are going to prove that after a suitable change of notation and the signs at a, b, c, d we have $3 \mid a+b+c$. This is plain if at least three of the numbers a, b, c, d are divisible by 3. Suppose that only two of them, say c and d, are divisible by 3. Then $a \equiv \pm 1 \pmod 3$ and $b \equiv \pm 1 \pmod 3$, whence for a suitable choice of the sign we have $3 \mid a \pm b$, so $3 \mid a \pm b + c$. Finally, if at least three of the numbers a, b, c, d, say a, b, c, are not divisible by 3, then for a suitable choice of the sign $\pm$ we have $3 \mid a \pm b \pm c$. Thus without any loss of generality we may assume that

$$a+b+c = 3z, \tag{28}$$

where z is an integer. But among three integers at least two are congruent mod 2; therefore, in addition we may assume that $a \equiv b \pmod 2$, whence it follows that $a+b = 2k$, where k is an integer, and so $a-b = 2(k-b) = 2y$, where y is an integer. But, it is easy to verify that the following identity holds:

$$3(a^2+b^2+c^2) = (a+b+c)^2+2\left(\frac{a+b}{2}-c\right)^2+6\left(\frac{a-b}{2}\right)^2,$$

whence

$$3(a^2+b^2+c^2) = (a+b+c)^2+2(k-c)^2+6y^2,$$

which, by (28), proves that $3 \mid k-c$; so $k-c = 3t$, where t is an integer. Hence, by (28), $a^2+b^2+c^2 = 3z^2+6t^2+2y^2$, and so, by (27), $n = d^2+2y^2+3z^2+6t^2$, and this completes the proof of the theorem of Jacobi. □

EXERCISES. 1. On the basis of Theorem 4 prove that every natural number which is divisible by 8 is the sum of the squares of eight odd integers.

PROOF. If n is a natural number, then, by Theorem 4, there exist four integers a, b, c, d such that

$$n-1 = a^2+b^2+c^2+d^2,$$

whence

$$8n = (2a-1)^2+(2a+1)^2+(2b-1)^2+(2b+1)^2+(2c-1)^2+(2c+1)^2+ +(2d-1)^2+(2d+1)^2. \quad \square$$

2. Prove that no natural number divisible by 8 is the sum of the squares of fewer than eight odd integers.

PROOF. As it is easy to prove, the sum of the squares of s odd numbers is of the form $8k+s$, where k is a non-negative integer. So, if the sum is divisible by 8, then $8 \mid s$, and thus $s \geqslant 8$. □

6. The sums of the squares of four natural numbers

As an immediate consequence of Theorem 4, we conclude that any natural number is the sum of the squares of four, or fewer, natural numbers. Using Gauss's theorem we now prove

THEOREM 5. *A natural number n is the sum of the squares of four natural numbers if and only if it does not belong to the sequence of the numbers* 1, 3, 5, 9, 11, 17, 29, 41, $4^h\cdot 2$, $4^h\cdot 6$, $4^h\cdot 14$, *where* $h = 0, 1, 2, \ldots$ (¹).

PROOF. We say that a natural number is S_m if it is the sum of the squares of m natural numbers. It is easy to prove that none of the numbers 1, 3, 5, 9, 11, 29, 41 is S_4. We prove this for 41, for instance. Suppose, to the contrary, that 41 is S_4, i.e. that $41 = a^2+b^2+c^2+d^2$, where a, b, c, d are natural numbers, and $a \geqslant b \geqslant c \geqslant d$. Hence $a^2 < 41 \leqslant 4a^2$, and so $4 \leqslant a \leqslant 6$. If $a = 6$, then $5 = b^2+c^2+d^2$, which is impossible. If $a = 5$, then $16 = b^2+c^2+d^2$, which again is impossible, since, as is easy to see,

---

(¹) G. Pall [1], p. 11. The truth of this theorem was conjectured by Descartes.

16 is not S_3. If $a = 4$, then $25 = b^2+c^2+d^2$, which is impossible, since 25 is not S_3. Consequently, 41 cannot be S_4.

Now, let m denote any of the numbers 2, 6, 14. Then m is of the form $4k+2$. Suppose that there exists a non-negative integer h such that $4^h m$ is S_4. Let h denote the least of such integers. Since 2, 6 and 14 are not S_4, $h \geqslant 1$. We then have $4^h m = a^2+b^2+c^2+d^2$, where a, b, c, d are natural numbers and the left-hand side of the equality is divisible by 8 because $h \geqslant 1$ and $m = 2(2k+1)$. From this we easily infer that each of the numbers a, b, c, d must be even. Thus $a = 2a_1, b = 2b_1, c = 2c_1, d = 2d_1$, where a_1, b_1, c_1, d_1 are natural numbers. Hence $4^{h-1}m = a_1^2+b_1^2+c_1^2+d_1^2$, which means that $4^{h-1}m$ is S_4 contrary to the definition of the number h. Thus we have proved that the number $4^h m$, where $m = 2, 6, 14$, is not S_4 for any non-negative integer h. This shows that the condition of Theorem 5 is necessary.

Now let n denote an odd natural number that satisfies the conditions of Theorem 5. Consequently, $n \neq 1, 3, 5, 9, 11, 17, 29, 41$. Since n is odd, it must be of one of the forms $8k+1$, $8k+3$, $8k+5$, $8k+7$.

Suppose that $n = 8k+1$. We are going to consider four cases $k = 4t, k = 4t+1$, $k = 4t+2$, $k = 4t+3$. If $k = 4t$, then $n = 32t+1$ and, since $n \neq 1$, we must have $t \geqslant 1$, and so $t = u+1$, where u is a non-negative integer. Hence $n = 32(u+1)+1 = 4(8u+6)+9$. By Gauss's theorem, the number $8u+6$ is the sum of the squares of three integers. Since $8u+6 = 2(4u+3)$ cannot be the sum of the squares of two integers, we see that $8u+6$ is S_3, whence it follows that the number $n = 2^2(8u+6)+3^2$ is S_4. If $k = 4t+1$, then $n = 32t+9$. Therefore, since $n \neq 9$ and $n \neq 41$, we have $t \geqslant 2$, so $t = u+2$ where u is an integer $\geqslant 0$. Hence $n = 32(u+2)+9 = 2^2(8u+6)+7^2$, whence, as above, we infer that n is S_4. If $k = 4t+2$, then $n = 32t+17$ and, by $n \neq 17$, we have $t \geqslant 1$, and so $t = u+1$, where u is an integer $\geqslant 0$. Hence $n = 32(u+1)+17 = 2^2(8u+6)+5^2$, whence n is S_4. If $k = 4t+3$, then $n = 32t+25 = 2^2(8t+6)+1^2$, whence n is S_4. Thus we see that the condition of Theorem 5 is sufficient provided $n = 8k+1$.

Now suppose that $n = 8k+3$. Since $n \neq 3$ and $n \neq 11$, we have $k \geqslant 2$, and so $k = t+2$, where t is a non-negative integer. We then have $n = 8(t+2)+3 = 8t+3+4^2$; therefore, in virtue of Gauss's theorem, which implies that the number $8t+3$ is the sum of the squares of three odd numbers, we conclude that n is S_4. The condition of Theorem 5 is thus sufficient also for the numbers $n = 8k+3$.

Further, suppose that $n = 8k+5$. We are going to consider four cases:

$k = 4t, k = 4t+1, k = 4t+2, k = 4t+3$. If $k = 4t$, then $n = 32t+5$ and, since $n \neq 5$, we have $t > 0$, so $t = u+1$, where u is a non-negative integer. Hence $n = 32(u+1)+5 = 2^2(8u+3)+5^2$, whence we infer that n is S_4. If $k = 4t+1$, then $n = 32t+13 = 2^2(8t+3)+1^2$, which shows that n is S_4. If $k = 4t+2$, then $n = 32t+21 = 2^2(8t+3)+3^2$, whence n is S_4. If $k = 4t+3$, then $n = 32t+29$ and, since $n \neq 29$, we have $t > 0$, so $t = u+1$, where $u \geqslant 0$, whence $n = 32(u+1)+29 = 2^2(8u+3)+7^2$, which shows that n is S_4. The condition of Theorem 5 is thus sufficient for the numbers $n = 8k+5$.

Finally, we consider $n = 8k+7$. Then, by Theorem 4, there exist integers a, b, c, d such that $n = a^2+b^2+c^2+d^2$. On the other hand, by Theorem 3, since $n = 8k+7$, none of the numbers a, b, c, d can be equal to zero. Thus n is S_4.

We have thus proved that *in order that an odd natural number be the sum of the squares of four natural numbers it is necessary and sufficient that it should not be any of the numbers* 1, 3, 5, 9, 11, 17, 29, 41. *This implies that any odd natural number* > 41 *is the sum of the squares of four natural numbers.*

Now let n denote an even natural number different from $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, where $h = 0, 1, 2, \ldots$ Let 4^h denote the highest power of the number 4 which divides the number n. We have $n = 4^h m$, where m is not divisible by 4. Consequently, $m = 4k+1$, $m = 4k+2$, or $m = 4k+3$.

If $m = 4k+1$ with even k, i.e. with $k = 2t$, then $m = 8t+1$, which, as proved above, is S_4, if, in addition, $m \neq 1, 9, 17, 41$. Then also $n = 4^h m$ is S_4. But, since n is even, in virtue of the fact that m is not divisible by 4, we must have $h > 0$. Clearly, 4 is S_4, $4 \cdot 17 = 68 = 1^2+3^2+3^2+7^2$, $4 \cdot 41 = 164 = 1^2+1^2+9^2+9^2$, whence $4^h \cdot 1 = 4(2^{h-1})^2$, $4^h \cdot 9 = 4(2^{h-1} \cdot 3)^2$, $4^h \cdot 17 = 4 \cdot 17(2^{h-1})^2$, $4^h \cdot 41 = 4 \cdot 41(2^{h-1})^2$ are all S_4. Thus we see that, if $m = 4k+1$ and k is even, then $n = 4^h m$ is S_4. If $m = 4k+1$ and k is odd, i.e. $k = 2t+1$, then $m = 8t+5$, as proved above, is S_4 provided $m \neq 5$ and $m \neq 29$. But $4 \cdot 5 = 20 = 1^2+1^2+3^2+3^2$, $4 \cdot 29 = 116 = 1^2+3^2+5^2+9^2$, whence, by the fact that m is odd, n is even and h is a natural number, we infer that both numbers are S_4. Thus we have proved that if $m = 4k+1$, then $n = 4^h m$ is S_4.

Suppose that $m = 4k+2$, then, if $k = 2t$, we have $m = 8t+2$. Since $n \neq 4^h \cdot 2$, and since $n = 4^h m$, we have $m \neq 2$, and so $t > 0$, i.e. $t = u+1$, where u is a non-negative integer. We then have $m = 8(u+1)+2 = 8u+6+2^2$. Since, as we have already learned, $8u+6$ is S_3, we infer that m is S_4, and consequently $n = 4^h m$ is also S_4. In the case of $k = 2t+1$ we have

$m = 8t+6$, and since $n \neq 4^h \cdot 6$ and $n \neq 4^h \cdot 14$, we must have $t \geqslant 2$; so $t = u+2$, where u is a non-negative integer. Hence $m = 8(u+2)+6 = 8u+6+4^2$, which, in virtue of the fact that $8u+6$ is S_3, implies that m is S_4, whence it follows that $n = 4^h m$ is also S_4. Thus we have proved that if $m = 4k+2$, then $n = 4^h m$ is S_4.

Finally, if $m = 4k+3$, then, in the case of $k = 2t$, we have $m = 8t+3$. But, as is shown above, for $m \neq 3$ and $m \neq 11$ the number $m = 8t+3$ is S_4. Thus, if $m = 4k+3$, then the number $n = 4^h m$ is S_4 provided $n \neq 4^h \cdot 3$, $n \neq 4^h \cdot 11$. But $4 \cdot 3 = 12 = 1^2+1^2+1^2+3^2$ and $4 \cdot 11 = 44 = 1^2+3^2+3^2+5^2$. Thus $n = 4^h m$, where $h > 0$, is S_4 because n is even and m odd. In the case of $k = 2t+1$ we have $m = 8t+7$, and so, as we know, m is S_4. This implies that $n = 4^h m$ is also S_4. Thus we have proved that, if $m = 4k+3$, then $n = 4^h m$ is S_4.

We sum up the results we have just proved in the statement that, if n is an even number different from $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, where $h = 0, 1, 2, \ldots$, then n is S_4. We have also proved that *an even natural number n is the sum of the squares of four natural numbers if and only if it is none of the numbers $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, where $h = 0, 1, 2, \ldots$*

This, combined with the results obtained for odd numbers, completes the proof of Theorem 5. □

Theorem 5 implies the following

COROLLARY. *The square of any natural number > 1, with the exception of 3^2, is the sum of the squares of four natural numbers.*

EXERCISE. Without using the theorem of Gauss, prove that any positive rational number is the sum of the squares of four positive rationals.

PROOF. Let r be a positive rational, $r = l/m$, where l and m are natural numbers. By Theorem 4 it follows that every natural number is the sum of the squares of four or fewer natural numbers. If $lm = a^2+b^2+c^2+d^2$, where a, b, c, d are natural numbers, then $r = l/m = (a/m)^2+(b/m)^2+(c/m)^2+(d/m)^2$, whence we see that r is the sum of the squares of four natural numbers. If $lm = a^2+b^2+c^2$, where a, b, c are natural numbers, then $r = l/m = (a/m)^2+(b/m)^2+(3c/5m)^2+(4c/5m)^2$. If $lm = a^2+b^2$, where a, b are natural numbers, then $r = l/m = (a/m)^2+(b/3m)^2+(2b/3m)^2+(2b/3m)^2$. Finally, if $lm = a^2$, where a is a natural number, then $r = l/m = 4(a/2m)^2$. Thus, in any case, r is the sum of the squares of four positive rational numbers. □

REMARK. It can be proved that each positive rational number is the sum of the squares of four different positive rationals, and that for any positive rational there are infinitely many such representations.

As it is proved in § 4, the numbers 2^n, where $n = 1, 2, \ldots$, and *a fortiori*, the numbers $4^h \cdot 2$, $h = 0, 1, 2, \ldots$, are not S_3. On the other hand, $3 = 1^2 + 1^2 + 1^2$, $9 = 1^2 + 2^2 + 2^2$, $11 = 1^2 + 1^2 + 3^2$, $17 = 2^2 + 2^2 + 3^2$, $29 = 2^2 + 3^2 + 4^2$, $41 = 1^2 + 2^2 + 6^2$, $4^h \cdot 6 = (2^h)^2 + (2^h)^2 + (2^{h+1})^2$, $4^h \cdot 14 = (2^h)^2 + (2^{h+1})^2 + (2^h \cdot 3)^2$ for $h = 0, 1, 2, \ldots$ Thus, by Theorem 5, we deduce

THEOREM 6. *A natural number n is the sum of the squares of three or four natural numbers if and only if n is none of the numbers* 1, 5, *and* $4^h \cdot 2$, *where* $h = 0, 1, 2, \ldots$

This, in consequence, gives the following

COROLLARY. *An odd natural number n is the sum of the squares of three or four natural numbers if and only if n is different from* 1 *and* 5.

This corollary is the basis of our proof of the following

THEOREM 7 (Hurwitz [2]). *The only natural numbers n for which n^2 is not the sum of the squares of three natural numbers are the numbers $n = 2^h$ and $n = 2^h \cdot 5$, where $h = 0, 1, 2, \ldots$*

PROOF. In § 4 we proved that, if k is not S_3, then the number $4k$ is not S_3. But, since the numbers 1 and 5^2 are not S_3, the numbers 4^h and $4^h \cdot 5^2$, $h = 0, 1, 2, \ldots$, are not S_3. Thus it remains to prove that, if n is a natural number $\neq 2^h$ and $\neq 2^h \cdot 5$, where $h = 0, 1, 2, \ldots$, then n^2 is S_3.

Suppose therefore that n is a natural number such that $n \neq 2^h$ and $n \neq 2^h \cdot 5$, where $h = 0, 1, 2, \ldots$ Let s be the greatest exponent for which 2^s divides n. We have $n = 2^s m$, where m is odd. Moreover, in virtue of the condition on n, m must be different from 1 and 5. From the corollary to Theorem 6 it follows that m is the sum of the squares of three or four natural numbers; $m = a^2 + b^2 + c^2 + d^2$, where a, b, c are natural numbers and d is a non-negative integer. Hence

$$m^2 = (a^2 + b^2 + c^2 + d^2)^2 = (a^2 + b^2 - c^2 - d^2)^2 + (2(ac + bd))^2 +$$
$$(2(ad - bc))^2 = (a^2 + b^2 - c^2 - d^2)^2 + (2(ad + bc))^2 + (2(ac - bd))^2.$$

Since m is odd, the equality $m = a^2 + b^2 + c^2 + d^2$ implies that among the numbers a, b, c, d either one or three numbers are odd, the remaining ones being even. Therefore the number $a^2 + b^2 - c^2 - d^2$ is odd, and so it is different from zero. Since a, b, c are natural numbers, $ac + bd$ and ad

$+bc$ are also natural numbers. We are going to prove that at least one of the numbers $ad-bc$, $ac-bd$ is different from zero. In fact, suppose that $ad = bc$ and $ac = bd$. Then $adc = bc^2$ and $acd = bd^2$, whence $bc^2 = bd^2$, and so, since $b > 0$, $c^2 = d^2$. Hence, in view of $c > 0$, $a = b$, whence $m = 2(a^2+c^2)$, which is impossible, since m is odd. Therefore either $ad-bc \neq 0$ or $ac-bd \neq 0$ (or both). Thus at least one of the sums written above gives a representation of the number m^2 as the sum of the squares of three natural numbers. We thus have $m^2 = x^2+y^2+z^2$, where x, y, z are natural numbers.

Hence, $n^2 = (2^s x)^2+(2^s y)^2+(2^s z)^2$, which proves that n^2 is S_3.

Theorem 7 is thus proved. ☐

By Theorem 7 it follows that *a natural number n is a principal diagonal of a rectangular parallelepiped whose edges are natural numbers if it is not of the form* 2^h or $2^h \cdot 5$, *where* $h = 0, 1, 2, \ldots$

From Theorem 7 it follows that for any odd natural number t different from 1 and 5 there exist natural numbers x, y, z such that $t^2 = x^2+y^2+z^2$. The question arises whether for every odd natural number t different from 1 and 5 there exist natural numbers x, y, z such that $(x, y, z) = 1$ and $x^2+y^2+z^2 = t^2$. As proved by A. Schinzel ([10], Corollary 1), the answer to this question is in the positive. (It is easy to prove that for even t there are no such x, y, z.) F. Steiger [1] has found 347 such systems x, y, z for $t \leqslant 100$. For example, $3^2 = 1^2+2^2+2^2$, $7^2 = 2^2+3^2+6^2$, $9^2 = 1^2+4^2+8^2 = 4^2+4^2+7^2$, $11^2 = 2^2+6^2+9^2$, $13^2 = 3^2+4^2+12^2$, $15^2 = 2^2+5^2+14^2 = 2^2+10^2+11^2$, $17^2 = 1^2+12^2+12^2 = 8^2+9^2+12^2$, $19^2 = 1^2+6^2+18^2 = 6^2+6^2+17^2 = 6^2+10^2+15^2$.

A. Schinzel ([10], Theorem 1) gives necessary and sufficient conditions for a natural number n to be representable in the form $x^2+y^2+z^2$, where x, y, z are natural numbers such that $(x, y, z) = 1$. The conditions however are somewhat complicated.

The problem of representing a natural number as the sum of the squares of four different integers has also been considered. We have namely the following theorem of G. Pall [1].

The only natural numbers that cannot be represented as the sums of four different squares $\geqslant 0$ *are the numbers* $4^h a$, *where* $h = 0, 1, 2, \ldots$, $a = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27, 31, 33, 37, 43, 47, 55, 67, 73, 97, 103, 2, 6, 10, 18, 22, 34, 58, 82$.

F. Halter-Koch [1] has enumerated all numbers that are not sums of four different positive squares.

7. Sums of $m \geqslant 5$ positive squares

By Theorem 5 any odd natural number > 41 is S_4. Therefore, if to any such number we add 1^2 or 2^2, we see that any even number > 42 and any odd number > 45 are S_5. Thus it remains to consider numbers $\leqslant 45$. By Theorem 5 numbers 4, 7, 10, 12, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44 are S_4. So, adding 1 or 4 to any of them we obtain numbers of S_5. There are still the numbers 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18 and 33 to be considered. It is easy to prove that none of them is S_5. We exemplify this by proving that 33 is not S_5. Suppose that 33 is S_5, i.e. that $33 = a^2+b^2+c^2+d^2+e^2$, where a, b, c, d, e are natural numbers such that $a \geqslant b \geqslant c \geqslant d \geqslant e$. Hence $a^2+4 \leqslant 33 \leqslant 5a^2$; so $6 < a^2 \leqslant 29$, which shows that $3 \leqslant a \leqslant 5$, whence $a = 3$ or 4 or 5. In the case of $a = 3$ the number $33-a^2 = 24 = 4 \cdot 6$ is S_4, contrary to Theorem 5. If $a = 4$, the number $33-a^2 = 17$ is S_4, which, as in the previous case, contradicts Theorem 5; the case of $a = 5$ gives $33-a^2 = 8 = 4 \cdot 2$ and this is also impossible, since, by Theorem 5, $4 \cdot 2$ is not S_4.

We have thus proved

THEOREM 8. *The only natural numbers that are not the sums of the squares of five natural numbers are the numbers* 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33.

Now let m be a natural number $\geqslant 6$. We are going to find the natural numbers $\leqslant m+13$ that are S_m. Suppose that n is such a number. Then there exist natural numbers $a_1, a_2, \ldots, a_m$ such that $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m$ and $n = a_1^2+a_2^2+\ldots+a_m^2$. Hence $a_1^2+(m-1) \leqslant n \leqslant m+13$, which implies $a_1^2 \leqslant 14$, and so $a_1 \leqslant 3$. Therefore $a_1 = 1$ or $a_1 = 2$ or $a_1 = 3$. In the case of $a_1 = 1$ (since $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m$) we have $a_1 = a_2 = \ldots = a_m = 1$, and so $m = n$. Suppose that $a_1 = 2$. If at least four of the numbers $a_2, a_3, \ldots, a_m$ are equal to 2, then $n \geqslant 5 \cdot 4+(m-5) = m+15$, contrary to the assumption that $n \leqslant m+13$. Consequently, at most three of the numbers $a_2, a_3, \ldots, a_m$ can be equal to 2. Therefore there are four possibilities: 1. none of them is equal to 2, and then $n = 4+(m-1) = m+3$; 2. one is equal to 2, then $n = 2 \cdot 4+(m-2) = m+6$; 3. two are equal to 2, then $n = 3 \cdot 4+(m-3) = m+9$; 4. three of the numbers $a_2, a_3, \ldots, a_m$ are equal to 2, then $n = 4 \cdot 4+(m-4) = m+12$. Thus all that remains to be considered is the case $a_1 = 3$. Then $n-9 = a_2^2+a_3^2+\ldots+a_m^2$. If $a_2 = 3$, then $n \geqslant 18+(m-2)$, contrary to the assumption that $n \leqslant m+13$. Consequently $a_2 \leqslant 2$. If $a_2 = 1$, then $a_3 = a_4 = \ldots = a_m = 1$; so $n = 3^2$

$+m-1 = m+8$. If $a_2 = 2$ and, if among the numbers $a_2, a_3, \ldots, a_m$ there are two or more numbers equal to 2, then $n \geqslant 3^2+2^2+2^2+(m-3) = m+14$, contrary to the assumption that $n \leqslant m+13$. Hence $a_3 = a_4 = \ldots = a_m = 1$, whence $m = 3^2+2^2+(m-2) = m+11$.

We have thus proved that among the natural numbers $\leqslant m+13$ only the numbers m, $m+3$, $m+6$, $m+8$, $m+9$, $m+11$, $m+\cdot 12$ are S_m.

Now we suppose that n is a natural number $> m+13$. If $n = m+28$, then, since $m \geqslant 6$, we have $n = m+28 = 2\cdot 3^2+4\cdot 2^2+(m-6)\cdot 1^2$, which shows that n is S_m. Suppose that $n \neq m+28$. Then $n-(m-5) > 18$ (since $n > m+13$) and $n-(m-5) \neq 33$. By Theorem 8 it follows that the number $n-(m-5)$ is S_5; so the number $n = n-(m-5)+(m-5)\cdot 1^2$ is S_m.

We sum up the results we have just obtained in

THEOREM 9 (Pall [1]). *If m is a natural number $\geqslant 6$, then the only positive integers that are not sums of the squares of m natural numbers are the numbers* $1, 2, 3, \ldots, m-1, m+1, m+2, m+4, m+5, m+7, m+10, m+13$.

By Theorems 8 and 9 we deduce that, if m is a natural number $\geqslant 5$, then any sufficiently large natural number is the sum of the squares of m natural numbers. This is not true for $m = 1, 2, 3, 4$, because there exist infinitely many natural numbers

1) which are not the squares of natural numbers (e.g. the numbers n^2+1, where $n = 1, 2, \ldots$),
2) which are not S_2 (e.g. the numbers of the form $4k+3$, where $k = 0, 1, 2, \ldots$),
3) which are not S_3 (e.g. the numbers of the form $8k+7$, where $k = 0, 1, 2, \ldots$),
4) which are not S_4 (e.g. the numbers of the form $4^h\cdot 2$, where $h = 0, 1, 2, \ldots$).

Equally, there exist infinitely many natural numbers which are not the sums of the squares of three or fewer natural numbers, e.g. numbers of the form $8k+7$, where $k = 0, 1, 2, \ldots$ However, by the theorem of Lagrange, any natural number is the sum of the squares of four or fewer natural numbers.

EXERCISES. 1. Prove that for any natural number m there exist infinitely many natural numbers which are S_i, $i = 1, 2, \ldots, m$, simultaneously.

PROOF. We show that any number of the form $(13k)^2$ greater than $m+13$ has this property. In fact, we have $n = (13k)^2 = (5k)^2+(12k)^2 = (3k)^2+(4k)^2+(12k)^2 = (2k)^2+(4k)^2+(7k)^2$

$+(10k)^2$. Thus we see that the number n is S_1, S_2, S_3 and S_4. If $i > 4$ and $i \leqslant m$, then we have $n = (13k)^2 > 33$ and $n > m+13$; so $n \ \cdot\ i+13$, which in virtue of Theorems 8 and 9 shows that n is S_i. ☐

REMARK. It can be proved that the least natural number which is S_1, S_2 and S_3 is 169. This number is S_i for all $i \leqslant 155$ and among the i's between 155 and 169 it is S_i only for $i = 157$, 158, 160, 161, 163, 166 and 169. The proof that 169 is S_{100} follows for instance from the formula $169 = 23 \cdot 2^2 + 77 \cdot 1^2$ or from the formula $169 = 8^2 + 2 \cdot 2^2 + 97 \cdot 1^2$.

2. Find the least natural number n which is S_i for any $i \leqslant 1000$.

SOLUTION. $n = 34^2$. In fact, since n is S_i, and so $n = k^2$, where k is a natural number, we have since n is S_{1000}, $k^2 \geqslant 1000$, and so $k \geqslant 32$. But, by Theorem 2, the numbers $32^2 = 2^{10}$ and $33^2 = (3 \cdot 11)^2$ cannot be S_2. However, $34^2 = 16^2 + 30^2 = 2^2 + 24^2 + 24^2$, whence we infer that 34^2 is S_1, S_2, S_3. By Theorem 5 we see that 34^2 is S_4 and by Theorem 8 it is S_5. Now a simple application of Theorem 9 shows that 34^2 is S_i provided $34^2 > i+13$ and $i \geqslant 6$. Therefore 34^2 is S_i for any $i \leqslant 1142$. An example of a representation of 34^2 as the sum of 1000 squares is $34^2 = 2 \cdot 8^2 + 2 \cdot 4^2 + 996 \cdot 1^2$.

3. Prove that the only natural numbers n such that n^2 is not S_5 are the numbers 1, 2, 3 and that the only natural numbers n for which n^2 is not S_6 are the numbers 1, 2, 4.

The proof follows immediately from Theorems 8 and 9.

8. The difference of two squares

THEOREM 10. *An integer k is representable as the difference of two squares if and only if k is not of the form $4t+2$, where t is an integer.*

PROOF. If a and b are two even numbers, then $a^2 - b^2$ is divisible by 4; if both a and b are odd, then $a^2 - b^2$ is divisible by 8; if, finally, one of the numbers a, b is even and the other is odd, then $a^2 - b^2$ is odd. We have thus proved that the condition of Theorem 10 is necessary.

Now suppose that an integer k is not of the form $4t+2$. Consequently, either k is odd or it is divisible by 4. If k is odd, then both $k-1$ and $k+1$ are even; so $(k-1)/2$ and $(k+1)/2$ are integers. We have

$$k = \left(\frac{k+1}{2}\right)^2 - \left(\frac{k-1}{2}\right)^2.$$

If k is divisible by 4, then

$$k = \left(\frac{k}{4}+1\right)^2 - \left(\frac{k}{4}-1\right)^2.$$

Thus we see that the condition is sufficient as well. This completes the proof of Theorem 10. ☐

The argument used to prove Theorem 10 will also prove the following

THEOREM 10^a. *Any natural number different from* 1 *and* 4, *which is not of the form* $4t+2$, *is the difference of the squares of two natural numbers.*

As is easy to prove, none of the numbers 1 and 4 can be represented as the difference of the squares of two natural numbers.

Our present aim is to determine all the representations of a given natural number n as the difference of the squares of two natural numbers.

Let n be a natural number different from 1 and 4 which is not of the form $4z+2$. Suppose that $n = x^2-y^2$, where x, y are natural numbers. We then have $n = (x+y)(x-y)$ and, if $d = x-y$, then d is a natural divisor of the number n less than the divisor $d' = x+y$, complementary to it. Moreover, the divisors d and d' are either both even or both odd because $d'-d = 2y$. Now let d denote an arbitrary natural divisor of the number n which is less than the complementary divisor $d' = n/d$ and such that d and d' are either both even or both odd. Then $x = \frac{d'+d}{2}$, $y = \frac{d'-d}{2}$ are natural numbers and $x^2-y^2 = \left(\frac{d'+d}{2}\right)^2 - \left(\frac{d'-d}{2}\right)^2 = dd' = n$. So $n = x^2+y^2$. We see that in this way all the representations of the number n as the difference of the squares of two natural numbers are obtained. Thus the number of the representations is equal to the number of natural divisors of the number n that are less than the complementary divisors, respectively, and such that the divisor and the divisor complementary to it are either both even or both odd. This, in particular, shows that any odd prime number has precisely one representation as the difference of the squares of two natural numbers, namely $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$. Another consequence is that, if an odd natural number is not the square of a natural number, then it has $d(n)/2$ different representations as the difference of the squares of two natural numbers. If the number n is a square, then it has $(d(n)-1)/2$ such representations. (By $d(n)$ we mean the number of the divisors of n.) This shows that odd primes are not the only numbers that have precisely one representation as the difference of squares of two natural numbers. The squares of odd primes have the same property; we have $p^2 = \left(\frac{p^2+1}{2}\right)^2$

$-\left(\frac{p^2-1}{2}\right)^2$. But any odd composite number that is not the square of a prime number has at least two representations as the difference of the squares of two natural numbers.

It is easy to prove that among the natural numbers divisible by 4 only the numbers of the form $4p$ or $4p^2$, where p is a prime $\geqslant 2$, have precisely one representation as the difference of the squares of natural numbers.

EXERCISE. Prove that for any natural number m there exists a natural number n which has precisely m representations as the difference of the squares of two natural numbers.

PROOF. For n we may set $n = 2^{2m+1}$. In fact, it has precisely m representations as the difference of the squares of two natural numbers because, as it is easy to see, the only such representations are $2^{2m+1} = (2^{2m-k}+2^{k-1})^2-(2^{2m-k}-2^{k-1})^2$, $k = 1, 2, \dots, m$. ☐

9. Sums of two cubes

It is easy to prove that any integer $\neq 0$ has a finite number $l \geqslant 0$ of representations as the sum of two cubes. Clearly, it suffices to prove this for natural numbers. The number of representations of a number as the sum of two non-negative cubes is, obviously, finite. Suppose that $n = x^3 + y^3$, where x, y are integers, $x > 0, y < 0$. We then have $n = (x+y)(x^2 - xy + y^2)$, where $-xy > 0$. But, since $x+y > 0$, whence $x+y \geqslant 1$, we have $x^2 - xy + y^2 \leqslant n$, which, in virtue of the fact that $-xy > 0$, proves that $x < \sqrt{n}$ and $0 < -y < \sqrt{n}$. From this we infer that the number of pairs x, y is finite.

Using the fact that the cube of an integer is congruent to 0, 1 or 8 (mod 9), one can easily prove that no integer of the form $9k \pm 4$, where k is an integer, can be the sum of three or fewer cubes. Consequently, there exist infinitely many natural numbers that are not representable as sums of two cubes. It is also easy to answer the question which are the prime numbers that are representable as sums of the cubes of two natural numbers. In fact, if $p = x^3 + y^3$, where x, y are natural numbers, then $p = (x+y)((x-y)^2 + xy)$, whence, since $x+y \geqslant 2$, we must have $p = x+y$ and $(x-y)^2 + xy = 1$, which shows that $x = y$ and $xy = 1$, and so $x = y = 1$ and $p = 2$. Thus we see that the number 2 is the only prime which can be represented as the sum of the cubes of two natural numbers.

Now we suppose that a prime p is the sum of the cubes of two integers one of which is not a natural number. Then prime p is the difference of the cubes of two natural numbers. Let $p = a^3-b^3$. We then have $p = (a-b)(a^2+ab+b^2)$, which implies $a-b = 1$ and $p = a^2+ab+b^2 = 3b(b+1)+1$. From this we see that, if a prime p is representable as the difference of the cubes of two natural numbers, then p must be of the form $p = 3b(b+1)+1$, where b is a natural number. On the other hand, if p is of this form, then $p = (b+1)^3-b^3$. Thus the primes of the form $3b(b+1)+1$ are precisely the ones which are representable as the differences of the cubes of natural numbers. We do not know whether there exist infinitely many primes of this form. (The answer in the positive follows from the conjecture H.) However, many primes of this form are known. For example, $7 = 2^3-1^3$, $19 = 3^3-2^3$, $37 = 4^3-3^3$, $61 = 5^3-4^3$, $127 = 7^3-6^3$.

THEOREM 11. *For any natural number m there exists a natural number n that is representable as the sum of the cubes of two integers in at least m different ways.*

PROOF. In § 15, Chapter II, we have proved that there exists an infinite sequence of systems x_k, y_k, z_k $(k = 1, 2, \ldots)$ of integers such that $(x_k, y_k) = 1$, $x_k^3+y_k^3 = 7z_k^3$ and $0 < |z_1| < |z_2| < \ldots$ Changing, if necessary, the signs of x_k and y_k we may assume that $z_k > 0$ for any $k = 1, 2, \ldots$

Let $n = 7z_1^3 z_2^3 \ldots z_m^3$, $a_k = \frac{z_1 z_2 \ldots z_m}{z_k} x_k$, $b_k = \frac{z_1 z_2 \ldots z_m}{z_k} y_k$ for $k = 1, 2, \ldots, m$. All a_k and b_k are integers and, moreover, $a_k^3+b_k^3 = n$.

If for some different indices i, j of the sequence $1, 2, \ldots, m$ we have $a_i = a_j$, then, since $z_k \neq 0$ for any $k = 1, 2, \ldots, m$, $x_i/z_i = x_j/z_j$, whence, in virtue of $(x_i, z_i) = (x_j, z_j) = 1$ we obtain $x_i = x_j$ and $z_i = z_j$, which is impossible. Similarly, if $a_i = b_j$, then $x_i/z_i = y_j/z_j$, which, in virtue of $(x_i, z_i) = (y_j, z_j) = 1$, is impossible. Thus we have obtained m different representations of the number n as a sum of the cubes of two integers. This completes the proof of Theorem 11. □

THEOREM 12. *Let n be a natural number that is neither the cube of a natural number not the cube of a natural number multiplied by 2. If n is representable as the sum of the cubes of two rational numbers, then n has infinitely many such representations.*

PROOF. Let r be the greatest integer for which r^3 divides n. Then $n = r^3a$, where a is a natural number which is not divisible by the cube of any natural number > 1. By assumption, a cannot be equal to 1 or 2. Suppose that n is the sum of the cubes of two rational numbers. If we reduce them to the same denominator, we may write $n = (u/t)^3 + (v/t)^3$, where u, v are integers and t is a natural number. Hence $u^3 + v^3 = a\,(rt)^3$. The numbers u, v are different from zero, since, by assumption, n is not the cube of a natural number, and so it cannot be the cube of a rational number. Thus $d = (u,v)$ is a natural number. Let $u = dx$, $v = dy$, where x, y are integers such that $(x, y) = 1$. We also have $d^3 \mid a\,(rt)^3$, whence, since a is not divisible by the cube of any natural number > 1, we easily infer that $d \mid rt$. and so $rt = dz$, where z is a natural number. We see that the numbers x, y, z satisfy the equation $x^3 + y^3 = az^3$. Thus, by Theorem 10, § 15, Chapter II, we deduce that this equation has infinitely many solutions in integers x, y, z with $(x, y) = (x, z) = (y, z) = 1$ and $z \neq 0$. For any such solution we have $nz^3 = a\,(rz)^3 = (rx)^3 + (ry)^3$, whence $n = (rx/z)^3 + (ry/z)^3$. Moreover, we see that different solutions give different representations of n as the sum of two cubes, because the fractions x/z and y/z are irreducible. Theorem 12 is thus proved. □

COROLLARY. *If r is a rational number which is neither the cube of a rational number nor the cube of a rational number multiplied by 2, and if r is representable as the sum of the cubes of two rational numbers, then r has infinitely many such representations.*

PROOF. Clearly, we may suppose that r is a positive rational number, i.e. that $r = l/m$, where l and m are natural numbers and $(l, m) = 1$. According to the hypothesis, there exist integers u, v and a natural number t such that

$$\frac{l}{m} = \left(\frac{u}{t}\right)^3 + \left(\frac{v}{t}\right)^3, \quad \text{whence} \quad lm^2 = \left(\frac{um}{t}\right)^3 + \left(\frac{vm}{t}\right)^3.$$

Thus the natural number lm^2 is the sum of the cubes of two rational numbers and it is neither the cube of a rational number nor the cube of a rational number multiplied by two, because, if it were, $r = l/m$ would be either the cube of a rational number or the cube of a rational number multiplied by two, contrary to the assumption. Thus, by Theorem 12, we see that the number lm^2 has infinitely many representations as the sum of the cubes of two rational numbers, which, in turn, implies that the number $r = lm^2/m^3$ has this property. This completes the proof of the corollary. □

10. The equation $x^3+y^3 = z^3$

Now we are going to present an elementary proof of Fermat Last Theorem for the exponent 3. The proof which we present here has been worked out by J. Browkin on the basis of ideas due to R. D. Carmichael [4], pp. 67–70.

THEOREM 13. *The equation*

(29) $$x^3+y^3 = z^3$$

is insolvable in integers x, y, $z \neq 0$.

LEMMA. *All the solutions of the equation*

(30) $$s^3 = a^2+3b^2$$

in integers a, b, s *such that* $(a, b) = 1$, s *is odd are given by the following formulae*

(31) $$s = \alpha^2+3\beta^2, \qquad a = \alpha^3-9\alpha\beta^2, \qquad b = 3\alpha^2\beta-3\beta^3,$$

where the numbers α, β *satisfy the conditions*

(32) $$\alpha \not\equiv \beta \pmod 2, \qquad (\alpha, 3\beta) = 1.$$

PROOF OF THE LEMMA. First we suppose that the integers α, β satisfy conditions (32). Let the numbers a, b, s be given by formulae (31). Then, using the identity

(33) $$(A^2+3B^2)^3 = (A^3-9AB^2)^2+3(3A^2B-3B^3)^2,$$

we easily verify that the numbers a, b, s satisfy equation (30). By (32) we infer that $(a, b) = \big(\alpha(\alpha^2-9\beta^2),\ 3\beta(\alpha^2-\beta^2)\big) = (\alpha^2-9\beta^2, \alpha^2-\beta^2)$ $= (8\beta^2, \alpha^2-\beta^2) = 1$ and that s is odd.

Suppose that integers a, b, s satisfy equation (30) and that $(a, b) = 1$ and s is odd. In order to prove the lemma we have to find integers α, β that satisfy conditions (31) and (32).

In order to do this we note that any prime divisor of the number s is of the form $6k+1$. In fact, if $p \mid s$, then, since s is odd, $p \geqslant 3$. If $p = 3$, then by (30), $3 \mid a^2$; so $3 \mid a$, and, again by (30), $9 \mid 3b^2$, whence $3 \mid b$, contrary to the assumption that $(a, b) = 1$. Thus we see that $p > 3$. Since $p \mid s$ and (a, b) $= 1$, by (30) we infer that $(b, p) = 1$, so $0 \equiv a^2+3b^2 \equiv b^2(a^2b^{p-3}+3) \pmod p$. Hence $(ab^{(p-3)/2})^2 \equiv -3 \pmod p$. This shows that -3 is a quadratic residue to the modulus p. As is known, this implies that p is of the form $6k+1$.

The construction of α, β can now be carried out by induction with respect to the number n of the prime factors of the integer s.

If $n = 0$, then, since $s^3 = a^2+3b^2 \geqslant 0$, we obtain $s = 1$. So $a = \pm 1$, $b = 0$. Thus the numbers α, β are defined by setting $\alpha = \pm 1$, $\beta = 0$. It is plain that conditions (31) and (32) are satisfied.

Now we suppose that the lemma is proved for a natural number $n \geqslant 0$. Let an integer s that has $n+1$ prime factors and two relatively prime integers a, b satisfy equation (30). Let p be a prime divisor of s; so $s = tp$, where t has n prime factors.

Since p is of the form $6k+1$, there exist integers α_1, β_1 such that $p = \alpha_1^2 + 3\beta_1^2$, where α_1, β_1 satisfy conditions (32). If $c = \alpha_1^3 - 9\alpha_1\beta_1^2$, $d = 3\alpha_1^2\beta_1 - 3\beta_1^3$, in virtue of identity (33), we obtain $p^3 = c^2+3d^2$ and, by (32), $(c, d) = 1$.

We have

(34) $$t^3p^6 = s^3p^3 = (a^2+3b^2)(c^2+3d^2) = (ac\pm 3bd)^2+3(ad\mp bc)^2.$$

Consider the product

(35) $$(ad-bc)(ad+bc) = (ad)^2-(bc)^2 = (a^2+3b^2)d^2-b^2(c^2+3d^2)$$
$$= t^3p^3d^2-b^2p^3 = p^3(t^3d^2-b^2).$$

If $p \mid ad-bc$ and $p \mid ad+bc$, then $p \mid 2ad$ and $p \mid 2bc$, whence, in virtue of the fact that p is odd, we obtain $p \mid ad$ and $p \mid bc$. But $p^3 = c^2+3d^2$ and $(c, d) = 1$. Hence $(p, c) = (p, d) = 1$ and so $p \mid a$ and $p \mid b$, contrary to $(a, b) = 1$.

Consequently, only one of the numbers $ad-bc$ and $ad+bc$ can be divisible by p. But, by (35), this number is divisible by p^3. Consequently, for the appropriate choice of the sign in the brackets at the end of (34) the number in the brackets is divisible by p^3. Since, in addition, the left-hand side of (34) is divisible by p^6, we see that the other number in the brackets on the right-hand side of (34) must be divisible by p^3. Therefore if the signs are suitably chosen,

(36) $$u = \frac{ac\pm 3bd}{p^3} \quad \text{and} \quad v = \frac{ad\mp bc}{p^3}$$

are integers. Thus formula (34) turns into the form

(37) $$t^3 = u^2+3v^2.$$

We solve (36) for a and b to find

$$a = uc+3vd \quad \text{and} \quad \pm b = ud-vc.$$

Hence, in view of $(a, b) = 1$, we infer that $(u, v) = 1$. In virtue of the inductive hypothesis and formulae (37), there exist integers α_2, β_2 which satisfy (32) and are such that

$$t = \alpha_2^2+3\beta_2^2, \qquad u = \alpha_2^3+9\alpha_2\beta_2^2, \qquad v = 3\alpha_2^2\beta_2-3\beta_2^3.$$

We write

$$\alpha = \alpha_1\alpha_2+3\beta_1\beta_2, \qquad \beta = \alpha_2\beta_1-\beta_2\alpha_1.$$

Then

$$\begin{aligned} s &= tp = (\alpha_1^2+3\beta_1^2)(\alpha_2^2+3\beta_2^2) = \alpha^2+3\beta^2, \\ a &= cu+3dv = (\alpha_1^3-9\alpha_1\beta_1^2)(\alpha_2^3-9\alpha_2\beta_2^2)+ \\ &\quad +3(3\alpha_1^2\beta_1-3\beta_1^3)(3\alpha_2^2\beta_2-3\beta_2^3) = \alpha^3-9\alpha\beta^2, \\ \pm b &= du-cv = (3\alpha_1^2\beta_1-3\beta_1^3)(\alpha_2^3-9\alpha_2\beta_2^2)- \\ &\quad -(\alpha_1^3-9\alpha_1\beta_1^2)(3\alpha_2^2\beta_2-3\beta_2^3) = 3\alpha^2\beta-3\beta^3. \end{aligned}$$

Changing, if necessary, the sign of β, we see that the numbers α, β satisfy equations (31). From this, since $(a, b) = 1$, we infer that the integers α, β satisfy (32). □

PROOF OF THEOREM 13. Suppose that numbers x, y, z satisfy equation (29) and, moreover, that they are chosen in such a way that the number $|xyz| \neq 0$ assumes the least possible value. Clearly any two of the numbers x, y, z are relatively prime, since otherwise a common divisor $d > 1$ of two of them would divide all the three and thus we could divide equation (29) throughout by d^3, which would produce a smaller solution.

It is very easy to verify that x, y, z are not all odd, and, by what we have proved above, only one of them is even. Consequently, we may assume that the number z is even and the numbers x, y are odd. So the numbers $x+y$ and $x-y$ are even, whence

(38) $$x+y = 2u, \qquad x-y = 2w.$$

Hence

(39) $$x = u+w, \qquad y = u-w.$$

By (39), in virtue of $(x, y) = 1$, since the numbers x, y are odd, we infer that $(u, w) = 1$ and $u \not\equiv w \pmod 2$. Substituting the values for x, y obtained from (39) in equation (29) we obtain

(40) $$2u(u^2+3w^2) = z^3.$$

If $(u, 3) = 1$, then, since $u \not\equiv w \pmod 2$, we have $(2u, u^2+3w^2) = 1$, so

(41) $$2u = t^3, \qquad u^2+3w^2 = s^3,$$

where s is an odd number and $(u, w) = 1$. In virtue of the lemma there exist integers α, β that satisfy conditions (32) and are such that $u = \alpha^3 - 9\alpha\beta^2$. Hence, by (41), $t^3 = 2u = 2\alpha(\alpha-3\beta)(\alpha+3\beta)$.

Now we verify without difficulty that any two of the numbers 2α, $\alpha-3\beta$, $\alpha+3\beta$ are relatively prime; so $2\alpha = \sigma^3$, $\alpha-3\beta = \tau^3$, $\alpha+3\beta = \varrho^3$, which gives the equality $\sigma^3 = \varrho^3+\tau^3$. But $|\varrho\sigma\tau|^3 = |t^3| = |2u| = |x+y| \neq 0$ and $|x+y| \leqslant |xyz| < |xyz|^3$, contrary to the assumption that $|xyz|$ is minimal.

If $3\,|\,u$, i.e. if $u = 3v$, then (40) can be rewritten in the form

$$18v(3v^2+w^2) = z^3, \tag{42}$$

whence, in view of $3v \not\equiv w \pmod 2$ and $(3v, w) = 1$, we obtain $(18v, 3v^2+w^2) = 1$; so

$$18v = t^3, \quad 3v^2+w^2 = s^3, \tag{43}$$

where s is odd and $(v, w) = 1$. In virtue of the lemma there exist integers α, β which satisfy conditions (32) and are such that $v = 3\beta\alpha^2 - 3\beta^3$. Hence, by (43), $t^3 = 18v = 27\cdot 2\beta(\alpha+\beta)(\alpha-\beta)$. It is easy to verify that any two of the numbers 2β, $\alpha+\beta$, $\alpha-\beta$ are relatively prime; so $2\beta = \sigma^3$, $\alpha+\beta = \tau^3$, $\alpha-\beta = \varrho^3$ which gives $\tau^3 = \sigma^3+\varrho^3$. But

$$|\varrho\sigma\tau|^3 = |\tfrac{1}{27}t^3| = |\tfrac{2}{3}v| = \tfrac{2}{9}|u| = \tfrac{1}{9}|x+y| \neq 0$$
$$\text{and} \quad \tfrac{1}{9}|x+y| \leqslant |xyz| \leqslant |xyz|^3,$$

contrary to the assumption that $|xyz|$ is minimal. Theorem 13 is thus proved. □

As an immediate consequence of Theorem 13 we obtain the following

COROLLARY. *The equation* $x^3+y^3 = z^3$ *has no solution in rational numbers* $\neq 0$.

EXERCISES. **1.** Prove that Theorem 13 is equivalent to the theorem stating that the equation $3x^2+1 = 4y^3$ has no solution in rational numbers except $x = \pm 1$, $y = 1$.

PROOF. If two rational numbers $x \neq \pm 1$ and y satisfy the equation $3x^2+1 = 4y^3$, then $u = (3x-1)/2$ is a rational number, $u \neq 1$ and $u \neq -2$. Moreover, $u^2+u+1 = 3y^2$, whence $y \neq 0$ (because the equation $u^2+u+1 = 0$ has no solution in rational numbers); consequently $(2+u)^3+(1-u)^3 = (3y)^3$, contrary to the corollary to Theorem 13. On the other hand, suppose that Theorem 13 is false. Then there exist rational numbers u, v different from zero and such that $u^3+v^3 = 1$ and $x = (u-v)/(u+v)$, $y = 1/(u+v)$ are rational numbers such that $3x^2+1 = 4y^3$. If $x = \pm 1$ and $y = 1$, then $u+v = 1$, $u-v = \pm 1$, whence $u = 0$ or $v = 0$, contrary to the definition of the numbers u, v. □

2. Prove that the equation $x^3+y^3 = z^3+1$ has infinitely many solutions in natural numbers x, y, z.

The proof follows immediately from the identity of Gérardin:

$$(9n^4)^3+(9n^3+1)^3 = (9n^4+3n)^3+1, \qquad n = 1, 2, \ldots$$

For example, if $n = 1$, $9^3+10^3 = 12^3+1$; if $n = 2$, $144^3+73^3 = 150^3+1$. We also have $64^3+94^3 = 103^3+1$.

3. Find three different natural numbers a, b, c such that the numbers $\sqrt[3]{a}, \sqrt[3]{b}, \sqrt[3]{c}$ are irrational and $\sqrt[3]{a}+\sqrt[3]{b} = \sqrt[3]{c}$.

ANSWER. $a = 2$, $b = 16$, $c = 54$.

11. Sums of three cubes

According to what we noticed at the beginning of § 9 no integer of the form $9k\pm 4$ is the sum of three of fewer cubes. On the other hand, we do not know whether every integer which is not of the form $9k\pm 4$ (where k is an integer) is the sum of three cubes. This, being easy to prove for any integer n, $-30 < n < 30$, turns to be rather difficult for the number 30; we do not know any representation of 30 as the sum of three cubes and we do not know whether such a representation exists.

V. L. Gardiner, R. B. Lazarus and P. R. Stein [1] have found the solutions of the equation $x^3+y^3-z^3 = \varepsilon k$ with $0 < k < 1000$ in integers x, y, z, ε satisfying $0 \leqslant x \leqslant y \leqslant 2^{16}$, $\varepsilon = \pm 1$. They have shown that there are no such solutions for $k = 30, 33, 39, 42, 52, 74, 75, 84$ and that for $k = 12$, $\varepsilon = 1$ there is precisely one solution $z = 11$, $y = 10$, $x = 7$.

This result, however, does not indicate whether there are other solutions of the equation in integers x, y, z among which at least two in their absolute value are greater than 2^{16}.

There, are some integers k for which we are able to prove that there are infinitely many representations of k as sums of three cubes. For example (cf. Mordell [4]):

$$0 = n^3+(-n)^3+0^3, \qquad 1 = (9n^4)^3+(1-9n^3)^3+(3n-9n^4)^3,$$
$$2 = (1+6n^3)^3+(1-6n^3)^3+(-6n^2)^3$$
$$\text{for any } n = 0, \pm 1, \pm 2, \ldots$$

For $k = 1$ there are representations of k as the sum of three cubes others than these given by the above formula. For example, $1 = 94^3+64^3+(-103)^3$. D. H. Lehmer [7] has proved that there exist infinitely many such representations (cf. Godwin [1]). In fact, let $x = 3^3t^4(2^43^2t^6-5)$, $y = -3t(6^4t^9+2^43^3t^6+3^3t^3-1)$, $z = 2^43^5t^9+2^33^4t^6-3^2t^3+1$.

It is easy to verify that for any t, $x^3+y^3+z^3 = 1$. If t is a natural number which is not divisible by 3, then the solution thus obtained is different from any of the solutions $9n^4$, $1-9n^3$, $3n-9n^4$, because, as one verifies directly, none of the numbers x, y, z is equal to $9n^4$, since y, z are not divisible by 9 and, if $x = 9n^4$, then in virtue of $3^3t^4 \mid x$, we obtain $3t \mid n$, so $n = 3ut$ (u an integer), whence $2^4 3^2 t^6 - 5 = 3^3 u^4$, which is impossible.

Substituting $t = 1$ we obtain $x = 3753$, $y = -5262$, $z = 4528$. For $t = -1$ we have $x = 3753$, $y = -2676$, $z = -3230$.

For $k = 2$ we do not know any representation of k as the sum of three cubes different from the one given above. We do not know any integer k not of the form $9t \pm 4$ for which it could be proved that it has only finitely many representations as the sum of three cubes. On the other hand, it is easy to prove that there exist infinitely many k's not of the form $9t \pm 4$ which are not representable as sums of the cubes of three natural numbers.

For $k = 3$ we know only four representations of k as the sum of three cubes; these are $(x, y, z) = (1, 1, 1), (-5, 4, 4), (4, -5, 4), (4, 4, -5)$ and we do not know whether there are any other such representations. As we shall see later, the number 3, like every other positive rational number, has infinitely many representations as the sum of the cubes of three positive rational numbers (cf. Theorem 14).

Representations of an integer in the form $x^3+y^3+2z^3$, where x, y, z are integers, have also been considered. To this end, Lal, Russel and Blundon [1] have proved that any natural number $\leqslant 1000$, except perhaps 19 of them (¹), admits at least one such representation. (For example, $13 = (-35)^3+(-62)^3+2(52)^3$, $20 = 63^3+(-3)^3+2(-50)^3$, $31 = 53^3+31^3+2(-44)^3$.) 76 is the least natural number about which we do not know whether it is of the form $x^3+y^3+2z^3$, where x, y, z are integers. The number 2, except the trivial decompositions $2 = t^3+(-t)^3+2\cdot 1^3$, has infinitely many such decompositions. This follows immediately from the identity $2 = (1-t-t^2)^3+(1+t-t^2)^3+2(t^2)^3$, valid for any integer t, this being the consequence of an identity due to B. Segre [1] (for $t = 2^m$ given by Niewiadomski [1]).

THEOREM 14. *Every positive rational number has infinitely many representations as the sum of three rational positive cubes.* (Cf. Hardy and Wright [1], pp. 197–199, Theorem 34.)

(¹) Three numbers out of 19 have been decomposed by J. C. Littlejohn (written communication from M. Lal).

PROOF. Let r be a given positive rational number. We define v as a rational number such that $\sqrt[3]{3r/2} < v < \sqrt[3]{3r}$. Let $u = (3r-v^3)/(3r+v^3)$, $s = v(1+u)$, $z = su$, $t = s/3(1-u^2)$, $x = s-t$, $y = t-z$.

Since $v < \sqrt[3]{3r}$, the number u is positive and less than 1; the numbers u, s, z, t are positive rationals, and x, y are rational numbers. In virtue of $v > \sqrt[3]{3r/2}$, we have $v^3 > \frac{3}{2}r$, whence $u = 6r/(3r+v^3)-1 < \frac{1}{3}$. Consequently, $3(1-u^2) > 1$, $s > t$ and $3u(1-u^2) < 1$, whence $z < 1$. Therefore $x > 0$ and $y > 0$. But

$$x^3+y^3+z^3 = (s-t)^3+(t-z)^3+z^3 = s^3-3(s^2-z^2)t+3(s-z)t^2$$

and

$$3(s^2-z^2) = 3s^2(1-u^2),$$

whence

$$3(s^2-z^2)t = s^3,$$

so

$$x^3+y^3+z^3 = 3(s-z)t^2 = 3s(1-u)t^2$$
$$= \frac{s^3(1-u)}{3(1-u^2)^2} = \frac{s^3}{3(1+u)(1-u^2)} = \frac{v^3(1+u)^2}{3(1-u^2)} = \frac{v^3(1+u)}{3(1-u)} = r.$$

In virtue of the fact that any rational number less than $\sqrt[3]{3r}$ and sufficiently close to $\sqrt[3]{3r}$ can be chosen as v, the number u and consequently the number $su = z$ can be arbitrarily small. This implies that the equation has infinitely many solutions in positive rational numbers. This completes the proof of Theorem 14. ☐

For $r = 3$, $v = 1$, the formulae above give the decomposition $3 = (\frac{2}{15})^3+(\frac{17}{75})^3+(\frac{36}{25})^3$.

Theorem 14 has the following two corollaries:

COROLLARY 1. *For any natural number n the equation $x^3+y^3+z^3 = nt^3$ has infinitely many solutions in natural numbers x, y, z, t such that $(x, y, z, t) = 1$.*

COROLLARY 2. *For any natural number $s \geqslant 3$ any positive rational number has infinitely many representations as the sum of the cubes of s positive rational numbers.*

If the proof of Theorem 14 is modified in the way that the number v we choose a little greater than $\sqrt[3]{3r}$, then $u < 0$, $1+u > 0$,

$1-u^2 > 0$, $u^2 < \frac{2}{3}$, so $s > 0$, $z < 0$, $t > 0$, $y > 0$, $x > 0$. This gives the proof of the following theorem:

Any positive rational number has infinitely many representations in the form $x^3+y^3-z^3$, *where* x, y, z *are rationals* > 0.

Applying this to the number $r+t^3$, where r, t are positive rationals, we obtain

THEOREM 15. *Any rational number has infinitely many representations in the form* $x^3+y^3-z^3-t^3$, *where* x, y, z, t *are positive rationals.*

12. Sums of four cubes

Several years ago I formulated the following conjecture:

C. *Any integer* g *has infinitely many representations in the form* $x^3+y^3-z^3-t^3$, *where* x, y, z, t *are natural numbers.*

The conjecture has been proved by Dem'yanenko [2] for the integers g with $-1000 \leqslant g \leqslant 1000$ and for all $g \not\equiv \pm 4 \pmod 9$. The proof is based on the following theorem due to L. J. Mordell [3]:

If $g = a^3+b^3-c^3-d^3$, *where* a, b, c, d *are integers*, $(a+b)(c+d) > 0$ *and* $a \neq b$ *or* $c \neq d$ *and, moreover, if the number* $(a+b)(c+d)$ *is not the square of a natural number, then Conjecture C is true for the number* g.

For $g = 0$ the truth of Conjecture C is an immediate consequence of the identity $0 = n^3+1^3-n^3-1^3$, for any $n = 1, 2, \ldots$

We are going to present here a straightforward verification of Conjecture C for $g = 1$ For this purpose it is sufficient to show that the equation

$$(t+13)^3+(u+14)^3-(t+3)^3-(u+17)^3 = 1$$

has infinitely many solutions in integers t, u. But this follows from the fact that the equation is satisfied for $t = u = 0$, and that, if is satisfied by the numbers t and u, then the numbers $t_1 = 11t+6u+173$, $u_1 = 20t+11u+315$ also satisfy it. For example, since $t = 0$ and $u = 0$ satisfy the equation, then also $t_1 = 173$, $u_1 = 315$ satisfy it and, moreover, $186^3+329^3-176^3-332^3 = 1$.

The fact that the equation $x^3+y^3-z^3-t^3 = 1$ has infinitely many solutions in natural numbers x, y, z, t implies that there exist infinitely many natural numbers n such that both n and $n+1$ are sums of two positive cubes.

If $g = 2$, an immediate proof of Conjecture C follows from the identity

$$2 = (9n^4)^3+1^3-(9n^3-1)^3-(9n^4-3n)^3 \quad \text{for any} \quad n = 1, 2, \ldots$$

In particular, for $n = 1$ we have $2 = 9^3+1^3-8^3-6^3$.

If $g = 3$, the truth of Conjecture C is a consequence of the identity

$$3 = (6n^3+1)^3+1^3-(6n^3-1)^3-(6n^2)^3 \quad \text{for} \quad n = 1, 2, \ldots$$

We also know positive integral solutions of the equation $x^3+y^3+z^3-t^3 = 1$, for example, $4^3+4^3+6^3-7^3 = 1$, $4^3+38^3+58^3-63^3 = 1$, $4^3+37^3+63^3-67^3 = 1$, and recently J. A. Gabowicz [1] has proved that the equation has infinitely many solutions in natural numbers.

On the other hand, it is easy to prove that there exist infinitely many solutions of the equation $x^3-y^3-z^3-t^3 = 1$ in natural numbers x, y, z, t. This is an immediate consequence of the identity

$$(6n^3+1)^3-1^3-(6n^2)^3-(6n^3-1)^3 = 1 \quad \text{for} \quad n = 1, 2, \ldots$$

As is shown by A. Mąkowski ([1], p. 121), the equation $x^3-y^3-z^3-t^3 = 2$ has infinitely many solutions in natural numbers. This fact follows immediately from the identity

$$(3n^3+1)^3-(3n^3-1)^3-(3n^2)^3-(3n^2)^3 = 2 \quad \text{for} \quad n = 1, 2, \ldots$$

The equation has also solutions that are not given by the above identity, for example $235^3-3^3-69^3-233^3 = 2$, $683^3-650^3-353^3-2^3 = 2$.

EXERCISE. Prove that there exist infinitely many natural numbers g for which each of the equations

$$g = x^3+y^3-z^3-t^3, \qquad g = x^3+y^3+z^3-t^3, \qquad g = x^3-y^3-z^3-t^3$$

has infinitely many solutions in natural numbers x, y, z, t.

PROOF. All $g = a^3-b^3$, where a and $b < a$ are arbitrary natural numbers, are such numbers. The proof follows immediately from the identities:

$$\begin{aligned} a^3-b^3 &= a^3+n^3-b^3-n^3, \\ a^3-b^3 &= a^3+((9n^3-1)b)^3+((9n^4-3n)b)^3-(9n^4b)^3, \\ a^3-b^3 &= (9n^4a)^3-((9n^3-1)a)^3-((9n^4-3n)a)^3-b^3. \end{aligned}$$

(cf. Schinzel and Sierpiński [2], pp. 26–27).

It is easy to prove that *any integer has infinitely many representations as the sum of five cubes.*

The identity

$$6t = (t+1)^3+(t-1)^3+(-t)^3+(-t)^3$$

shows that any integer divisible by 6 is the sum of four cubes. In order to prove that any integer has infinitely many representations as the sum of five cubes it is sufficient to show that for any integer there exists an arbitrarily large natural number such that the difference between the integer and the cube of the natural number is divisible by 6.

Let g denote an arbitrary integer, r the remainder left by g divided by 6. Then $g = 6k+r$. For any natural number n we have $6k+r-(6n+r)^3 \equiv r-r^3 \equiv 0 \pmod{6}$ so $6 \mid g-(6n+r)^3$.

13. Equal sums of different cubes

In connection with Theorem 13 it seems interesting to know which natural numbers m and $n \geqslant m$ are such that the equation

$$x_1^3+x_2^3+\ldots+x_m^3 = y_1^3+y_2^3+\ldots+y_n^3 \tag{44}$$

has solution in different natural numbers $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n$. It is clear that there are no solutions for $n = m = 1$. Theorem 13 implies that in the case of $m = 1$, $n = 2$ there are no solutions either. We prove

THEOREM 16. *In order that equation* (44), *where n, m are natural numbers, $n \geqslant m$, be solvable in different natural numbers $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n$ it is necessary and sufficient that neither $m = n = 1$ nor $m = 1$, $n = 2$* (cf. Sierpiński [24]).

All that we have to prove is the sufficiency of the condition.

LEMMA. *For any natural number $n > 2$ there exists a natural number whose cube is the sum of n different positive cubes.*

PROOF OF THE LEMMA. The formulae $6^3 = 3^3+4^3+5^3$ and $13^3 = 5^3+7^3+9^3+11^3$ prove the lemma for $n = 3$ and $n = 4$. Suppose that the lemma is true for a natural number $n > 2$. Then there exist natural numbers $a_1 < a_2 < \ldots < a_n < a_0$ such that $a_0^3 = a_1^3+a_2^3+\ldots+a_n^3$. Hence

$$(6a_0)^3 = (3a_1)^3+(4a_1)^3+(5a_1)^3+(6a_2)^3+(6a_3)^3+\ldots+(6a_n)^3$$

and, moreover, $3a_1 < 4a_1 < 5a_1 < 6a_2 < \ldots < 6a_n$, which proves the truth of the lemma for $n+2$. Thus we see that the assumption that the lemma is true for a natural number n implies that the lemma is true for $n+2$. This, combined with the fact that the lemma is proved to be true for $n = 3$ and $n = 4$, gives the proof of the lemma for any natural number $n > 2$. □

The lemma implies the following

COROLLARY. *Theorem* 16 *is true for any natural numbers m, n with $m > 3$, $n > 3$.*

PROOF OF THE COROLLARY. If $m > 3$ and $n > 3$, then, by the lemma, there exist natural numbers $b_1 < b_2 < \ldots < b_{n-1} < a_1$ such that $a_1^3 = b_1^3+b_2^3+\ldots+b_{n-1}^3$ and numbers $a_2 < a_3 < \ldots < a_m < b_n$ such that $a_2^3+a_3^3+\ldots$

$+a_m^3 = b_n^3$. Moreover, we may assume that $a_2 > a_1$, since, if it is not already true, we replace each of the numbers $a_2, a_3, \ldots, a_m, b_n$ by the product of its multiplication by the number a_1+1. Therefore the numbers $a_1, a_2, \ldots, a_m$, $b_1, b_2, \ldots, b_n$ are different. Adding together the equalities obtained above we see that $a_1^3+a_2^3+\ldots+a_m^3 = b_1^3+b_2^3+\ldots+b_n^3$, and this is what was to be proved in order to verify Theorem 16 for the numbers m and n. The corollary is thus proved. In order to obtain Theorem 16 in its whole generality it remains to prove that it is valid for $m = 2$ and $m = 3$ and any $n \geqslant m$.

If $m = 2$, $n = 2, 3, 4, 5$, the truth of Theorem 16 follows from the formulae

$$9^3+10^3 = 1^3+11^3, \quad 7^3+8^3 = 1^3+5^3+9^3,$$
$$6^3+36^3 = 4^3+5^3+27^3+30^3, \quad 26^3+28^3 = 2^3+3^3+4^3+5^3+34^3.$$

If $m = 2$ and $n > 5$, then, by the lemma, there exist natural numbers $b_1 < b_2 < \ldots < b_{n-3} < a_1$ such that $a_1^3 = b_1^3+b_2^3+\ldots+b_{n-3}^3$, whence $a_1^3+(6a_1)^3 = (3a_1)^3+(4a_1)^3+(5a_1)^3+b_1^3+b_2^3+\ldots+b_{n-3}^3$, which, by $a_1 < 3a_1 < 4a_1 < 5a_1 < 6a_1$ proves the theorem for n and m.

If $m = 3$, $n = 3, 4$ the truth of Theorem 16 follows from the formulae

$$1^3+12^3+15^3 = 2^3+10^3+16^3,$$
$$12^3+13^3+14^3 = 3^3+9^3+10^3+17^3.$$

If $m = 3$, $n > 4$, then, by the lemma, there exist natural numbers $b_1 < b_2 < \ldots < b_{n-2} < a_1$ such that $a_1^3 = b_1^3+b_2^3+\ldots+b_{n-2}^3$, whence $a_1^3+(2a_1)^3+(16a_1)^3 = (9a_1)^3+(15a_1)^3+b_1^3+b_2^3+\ldots+b_{n-2}^3$, and so, by $a_1 < 2a_1 < 9a_1 < 15a_1 < 16a_1$, the truth of Theorem 16 for the numbers m, n follows.

Theorem 16 is thus proved. □

14. Sums of biquadrates

In virtue of Fermat Last Theorem for the exponent 4 (cf. Chapter II, § 6) there is no biquadrate that is the sum of two positive biquadrates. According to the conjecture of Euler, there is no biquadrate which is the sum of three positive biquadrates either. However, there are biquadrates which are sums of four, five or six biquadrates. For example, $353^4 = 30^4+120^4+272^4+315^4$, $15^4 = 4^4+6^4+8^4+9^4+14^4$, $91^4 = 14^4+24^4+34^4+49^4+58^4+84^4$.

THEOREM 17. *For any natural number $n > 3$ there exists a biquadrate which is the sum of n different positive biquadrates.*

PROOF. Let S denote the set of the natural numbers $n > 1$ for which there exists a biquadrate that is the sum of n different positive biquadrates. As we have just shown numbers 4, 5, 6 belong to the set S. We now prove that if numbers n, m belong to S, then the number $m+n-1$ also belongs to S. In fact, if m and n belong to S, then there exist natural numbers $a_1 < a_2 < \ldots < a_m < a_0$ and $b_1 < b_2 < \ldots < b_n < b_0$ such that

$$a_0^4 = a_1^4+a_2^4+\ldots+a_m^4, \qquad b_0^4 = b_1^4+b_2^4+\ldots+b_n^4.$$

Hence

$$(a_0 b_0)^4 = (a_1 b_1)^4+(a_1 b_2)^4+\ldots$$
$$\ldots+(a_1 b_n)^4+(a_2 b_0)^4+(a_3 b_0)^4+\ldots+(a_m b_0)^4$$

and, moreover, $a_1 b_1 < a_1 b_2 < \ldots < a_1 b_n < a_2 b_0 < a_3 b_0 < \ldots < a_m b_0$. This shows that the number $m+n-1$ belongs to the set S. Now the proof is almost over, we simply notice that if a set S of natural numbers is such that the numbers 4, 5 belong to S and that together with any natural numbers m and n of S the number $m+n-1$ is in S, then S contains any natural number $\geqslant 7$. In fact, since 4 and 5 belong to S, then $4+4-1 = 7$, $5+4-1 = 8$, $5+5-1 = 9$ belong to S. By simple induction we verify that, if m belongs to S, then $m+3k$, where $k = 1, 2, \ldots$, is in S (this is because $m+3k = m+3(k-1)+4-1$). Consequently, the set S contains every number of the form $7+3k$, $8+3k$, $9+3k$, when $k = 0, 1, 2, \ldots$, that is S contains any natural number $\geqslant 7$. Since the numbers 4, 5, 6 belong to S, we see that S contains every natural number > 3. Theorem 17 is thus proved. □

We know some natural numbers which have two different representations as sums of two positive biquadrates. For example, $133^4+134^4 = 59^4+158^4$. However, we do not know any natural number which has more than two different representations as the sum of two positive biquadrates, provided representations that differ only in the order of the summands are regarded as identical.

The following equality holds $8^4+9^4+17^4 = 3^4+13^4+16^4$.

We thereby note that the identity

$$4^4 255^4 x = (8(255+2x))^4-(8(255-2x))^4+(32x-255)^4-(32x+255)^4$$

implies that any rational number is an algebraic sum of four rational biquadrates.

It can be proved that for any natural number $n \geqslant 4$ there exists a fifth power that is the sum of the fifth powers of n different natural numbers. For example, $144^5 = 27^5+84^5+110^5+133^5$, $12^5 = 4^5+5^5+6^5+7^5+9^5+11^5$, $92^5 = 2^5+9^5+11^5+22^5+51^5+58^5+89^5$, $32^5 = 3^5+6^5+7^5+8^5+10^5+11^5+13^5+14^5+15^5+16^5+18^5+31^5$ (cf. Lander and Parkin [2] and A. S. Bang [1]). According to P. Erdős, it can be proved that for any natural number m there exists a natural number k_m such that for any natural number $n > k_m$ there exists a natural number $l_{n,m}$ such that any natural number greater than $l_{n,m}$ is the sum of n different numbers each of which is a positive mth power.

15. Waring's theorem

In 1770 Waring stated without proof the following theorem:

For any exponent s there exists a natural number k such that any natural number n is the sum of k non-negative s-th powers.

This theorem was proved by D. Hilbert in 1909. An elementary proof of Waring's theorem, due to Yu. V. Linnik [2] and based on the idea of L. Schnirelman, is presented in a book of A. Ya. Khinchin [1].

For $s = 1$ Waring's theorem is true but irrelevant. If $s = 2$, Theorem 4 (of Lagrange) provides an evaluation for k as $k = 4$. For $s = 3$ Waring claimed that k can be assumed to be equal to 9, i.e. that any natural number is the sum of nine or fewer positive cubes. It was not until 1909 that A. Wieferich proved it true. For $s = 4$ Waring stated that $k = 19$ is good. This has been proved very recently (not in an elementary way) by R. Balasubramanian, F. Dress and J.-M. Deshonilles [1].

We are going to give an elementary proof that k can be assumed to be equal to 50 (cf. Theorem 18).

For a natural number s we denote by $g(s)$ the least natural number k such that any natural number is the sum of k or less sth powers. Waring's theorem asserts that for any s the natural number $g(s)$ exists. We prove that

$$g(s) \geqslant 2^s + [(\tfrac{3}{2})^s] - 2, \qquad s = 1, 2, \ldots \tag{45}$$

Let

$$n = 2^s[(\tfrac{3}{2})^s] - 1. \tag{46}$$

Clearly, n is a natural number, and, since $[x] \leqslant x$, we have

$$n < 3^s. \tag{47}$$

It follows from the definition of $g(s)$ that there exist non-negative integers x_i $(i = 1, 2, \dots, g(s))$ such that

$$n = x_1^s + x_2^s + \dots + x_{g(s)}^s. \tag{48}$$

By (47), any number x_i $(i = 1, 2, \dots, g(s))$ must be less than 3. Consequently, the numbers x_i can take only the three values, 0, 1 and 2. Suppose that among the x_i's there are k different numbers equal to 2, l equal to 1, and r equal to 0. Plainly, k, l, r are non-negative integers and

$$g(s) = k + l + r \geqslant k + l \tag{49}$$

with

$$n = 2^s k + l. \tag{50}$$

Hence $n \geqslant 2^s k$, and, since, by formula (46), $n < 2^s[(\frac{3}{2})^s]$, we obtain $k < [(\frac{3}{2})^s]$, i.e.

$$k \leqslant [(\tfrac{3}{2})^s] - 1. \tag{51}$$

In virtue of (50), we have $l = n - 2^s k$, and so

$$k + l = k + n - 2^s k = n - (2^s - 1)k. \tag{52}$$

Since s is a natural number, $2^s - 1$ is also a natural number; we multiply (51) by it to obtain

$$(2^s - 1)k \leqslant (2^s - 1)([(\tfrac{3}{2})^s] - 1).$$

Hence, by (49), (52) and (46).

$$g(s) \geqslant k + l \geqslant n - (2^s - 1)([(\tfrac{3}{2})^s] - 1) = 2^s + [(\tfrac{3}{2})^s] - 2,$$

which proves (45).

If $s = 2$, inequality (45) gives $g(2) \geqslant 2^2 + [\frac{9}{4}] - 2 = 4 + 2 - 2$, and so $g(2) \geqslant 4$. But, as we know, $g(2) = 4$. If $s = 3$, (45) shows that $g(s) \geqslant 2^3 + [\frac{27}{8}] - 2 = 9$. There exist natural numbers, for example 23, which are not representable as sums of eight non-negative cubes. As we have already mentioned, Wieferich proved that $g(3) = 9$.

If $s = 4$, (45) gives the inequality $g(4) \geqslant 2^4 + [\frac{81}{16}] - 2 = 19$. By (46), there exist natural numbers (e.g. 79) which are not representable as sums of 18 non-negative biquadrates. Balasubramanian, Dress and Deshonilles have proved that $g(4) = 19$.

If $s = 5$, inequality (45), by a simple calculation, gives $g(5) \geqslant 37$. J. R. Chen [1] has proved that $g(5) = 37$.

L. E. Dickson [4], [5] (cf. Pillai [3]) has proved that the formula

$$g(s) = 2^s + [(\tfrac{3}{2})^s] - 2$$

is valid for $6 \leqslant s \leqslant 400$, (actually, this is true also for $s \leqslant 5$). K. Mahler [1] has proved that the above formula is valid for any sufficiently large number s and R. M. Stemmler [1] has verified its validity for $400 < s \leqslant 200000$.

For a natural number s denote by $G(s)$ the least natural number k such that all sufficiently large natural numbers (i.e. all numbers with at most a finite number of exceptions) are representable by k non-negative sth powers. It has been proved that

$$G(2) = 4, \qquad G(3) \leqslant 7\,(^1), \qquad G(4) = 16, \qquad G(5) \leqslant 21,$$
$$G(6) \leqslant 31$$

(cf. Davenport [1] and Vaughan [1], [2]).

Now we are going to present an elementary proof that $g(4) \leqslant 50$.

Accordingly we recall the identity of E. Lucas (found in 1876)

$$(53) \quad \begin{aligned} 6(x_1^2+x_2^2+x_3^2+x_4^2)^2 = {} & (x_1+x_2)^4+(x_1-x_2)^4+(x_1+x_3)^4+ \\ & +(x_1-x_3)^4+(x_1+x_4)^4+(x_1-x_4)^4+ \\ & +(x_2+x_3)^4+(x_2-x_3)^4+(x_2+x_4)^4+ \\ & +(x_2-x_4)^4+(x_3+x_4)^4+(x_3-x_4)^4. \end{aligned}$$

Let n be a natural number divisible by 6, i.e. $n = 6m$, where m is a natural number. In virtue of Theorem 4, we have $m = a^2+b^2+c^2+d^2$, where a, b, c, d are non-negative integers. Hence $n = 6a^2+6b^2+6c^2+6d^2$. But, in virtue of Theorem 4, there exist non-negative integers x_1, x_2, x_3, x_4 such that $a = x_1^2+x_2^2+x_3^2+x_4^2$. Hence, by (53), $6a^2 = a_1^4+a_2^4+\ldots+a_{12}^4$, where a_i $(i = 1, 2, \ldots, 12)$ are non-negative integers. We represent each of the numbers $6b^2$, $6c^2$, $6d^2$ in a similar way as the sum of twelve biquadrates. From this we infer that the number $n = 6m$ is the sum of 48 biquadrates.

Thus we have proved that any natural number divisible by 6 is the sum of 48 biquadrates.

Any natural number $\leqslant 95$ is representable in the form 2^4k+r, where $0 \leqslant k \leqslant 5$, $0 \leqslant r \leqslant 15$, and so it is the sum of 20 biquadrates. Consequently, to complete the proof we may suppose that the number n is greater than 95. Then $n = 6m+r$, where $m > 15$ and $0 \leqslant r \leqslant 5$. The

---

(1) This was proved by Yu. V. Linnik [1] in 1942; a simpler proof is given by G. L. Watson [1], see also McCurley [1].

numbers m, $m-2$, $m-13$ are positive and so, for $r = 0, 1, 2, \ldots, 5$ we have $n = 6m$, $n = 6m+1^4$, $n = 6m+1^4+1^4$, $n = 6(m-13)+3^4$, $n = 6(m-2)+2^4$, $n = 6(m-2)+1^4+2^4$, respectively. Hence, in virtue of what we have proved above, we see that, since any natural number divisible by 6 is the sum of 48 biquadrates, every natural number is the sum of 50 biquadrates. Thus in an elementary way we have proved

THEOREM 18. *Every natural number is the sum of* 50 *biquadrates.*

Using the theorem of Gauss one can elementarily prove that $g(4) \leqslant 30$ (cf. Dress [1]).

For any natural number s we denote by $v(s)$ the least natural number k such that any natural number is the algebraic sum of k numbers each of which is the sth power of an integer.

It is easy to prove that $v(2) = 3$ and that $4 \leqslant v(3) \leqslant 5$, however we do not know whether $v(3)$ is equal to 4 or to 5. It is proved that $9 \leqslant v(4) \leqslant 10$, $5 \leqslant v(5) \leqslant 10$.

Now we are going to prove that for any natural number s the number $v(s)$ exists. To this aim we start with the identity of P. Tardy [1] (cf. Dickson [7], vol. II, pp. 723, 728)

$$\sum_{\alpha_1,\alpha_2,\ldots,\alpha_s} (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_s}\big((-1)^{\alpha_1}x_1+(-1)^{\alpha_2}x_2+\ldots+(-1)^{\alpha_s}x_s\big)^s = s!2^s x_1 x_2 \ldots x_s,$$

where s is a natural number, and the summation on the left-hand side extends all over the 2^s sequences $\alpha_1, \alpha_2, \ldots, \alpha_s$ the terms of which are 0 and 1.

Hence, for $x_1 = x_2 = \ldots = x_s = 1$, we deduce that every integer divisible by $s!2^s$ is an algebraic sum of 2^s sth powers. Therefore, since any integer is of the form $s!2^s k \pm r$, where k, r are integers and $0 \leqslant r \leqslant s!2^{s-1}$, we see that any integer is an algebraic sum of $2^s + s!2^{s-1}$ sth powers. This proves that

$$v(s) \leqslant 2^s + s!2^{s-1}, \qquad \text{for any } s = 1, 2, \ldots$$

CHAPTER XII

SOME PROBLEMS OF THE ADDITIVE THEORY OF NUMBERS

1. Partitio numerorum

Leibniz and Bernoulli and later on Euler were the first to consider the problem of establishing the number g_n of all possible representations of an arbitrary natural number n as the sum of non-increasing natural numbers. This problem is known under the name *partitio numerorum.*

Here are the initial ten values of the function g_n: $g_1 = 1$, $g_2 = 2$, $g_3 = 3$, $g_4 = 5$, $g_5 = 7$, $g_6 = 11$, $g_7 = 15$, $g_8 = 22$, $g_9 = 30$, $g_{10} = 42$.

Mac Mahon has found that $g_{100} = 1905692292$ and $g_{200} = 3972999029388$.

It can be proved that the numbers g_n are the coefficients of the expansion into a power series of the function

$$\prod_{n=1}^{\infty} \frac{1}{1-x^n} = 1 + \sum_{n=1}^{\infty} g_n x^n \quad \text{for} \quad |x| < 1.$$

Let h_n be the number of representations of a number n as the sum of increasing natural numbers. It is easy to prove that, for $|x| < 1$,

$$\prod_{n=1}^{\infty} (1+x^n) = 1 + \sum_{n=1}^{\infty} h_n x^n.$$

The numbers g_n ($n = 1, 2, \ldots$) satisfy the inductive identity

$$ng_n = \sigma(n) + g_1 \sigma(n-1) + g_2 \sigma(n-2) + \ldots + g_{n-1} \sigma(1),$$

which may serve as a rule for finding g_n's (cf. Vahlen [1]).

Here are the initial ten values of the function h_n: $h_1 = 1$, $h_2 = 1$, $h_3 = 2$, $h_4 = 2$, $h_5 = 3$, $h_6 = 4$, $h_7 = 5$, $h_8 = 6$, $h_9 = 8$, $h_{10} = 10$.

Denote by k_n the number of all possible decompositions of a natural number n into the sum of natural numbers, where two decompositions are considered as different also if they differ only in the order of the summands.

Easy induction shows that

$$k_n = 2^{n-1} \quad \text{for any } n = 1, 2, \ldots$$

Thus, in particular, the number 4 has eight different decompositions into the sum of natural numbers:

$$4 = 3+1 = 1+3 = 2+2 = 2+1+1 = 1+2+1 = 1+1+2$$
$$= 1+1+1+1.$$

Finally, let l_n denote the number of all possible decompositions of a natural number n into the sum of non-decreasing odd natural numbers. Then, for $|x| < 1$, we have

$$\prod_{n=1}^{\infty} \frac{1}{1-x^{2n-1}} = 1 + \sum_{n=1}^{\infty} l_n x^n.$$

It is worth-while to mention that it can be proved that the equality $l_n = h_n$ holds for any $n = 1, 2, \ldots$

Let q_n be the function which assigns to a natural number n the number of partitions of the set of n elements into non-void disjoint subsets, two partitions that differ only in the order of the parts being regarded as identical.

The initial values of this function are $q_1 = 1, q_2 = 2, q_3 = 5, q_4 = 15, q_5 = 52$.

We have the following formula for q_n (Whitworth [1], p. 88).

$$e^{e^x - 1} = \sum_{n=1}^{\infty} q_n x^n/n!.$$

We also have (Rota [1], where a complete bibliography is given)

$$q_{n+1} = 1 + \sum_{k=1}^{n} \binom{n}{k} q_k.$$

The number of different representations of an integer as the sum reduced with respect to the modulus m of different numbers of the sequence $1, 2, \ldots, m-1$ has also been considered. M. A. Stern [1] has proved that, if p is an odd prime, then any residue to p has precisely $(2^{p-1} - 1)/p$ such representations, where the summands are $1, 2, \ldots, p-1$.

For example, if $p = 5$,

$$0 \equiv 1+4 \equiv 2+3 \equiv 1+2+3+4 \pmod 5,$$
$$1 \equiv 1 \equiv 2+4 \equiv 1+2+3 \pmod 5,$$
$$2 \equiv 2 \equiv 3+4 \equiv 1+2+4 \pmod 5,$$
$$3 \equiv 3 \equiv 1+2 \equiv 1+3+4 \pmod 5,$$
$$4 \equiv 4 \equiv 1+3 \equiv 2+3+4 \pmod 5.$$

2. Representations as sums of n non-negative summands

We now prove that if n and k are two given natural numbers, then the number $F_{n,k}$ of all possible representations of the number k as the sum of n nonnegative integers, where two representations that differ in the order of the summands are also regarded as different, is $\binom{n+k-1}{k}$.

In fact, we have $F_{1,k} = 1 = \binom{k}{k}$. Suppose that for a natural number n the formula $F_{n,k} = \binom{n+k-1}{k}$ is valid for any $k = 1, 2, \ldots$ Then it is easy to see that

$$F_{n+1,k} = F_{n,k}+F_{n,k-1}+F_{n,k-2}+ \ldots +F_{n,1}+1$$
$$=\binom{n+k-1}{k}+\binom{n+k-2}{k-1}+\binom{n+k-3}{n-2}+\ldots+\binom{n}{1}+1.$$

For any two natural numbers n and k the identity

$$\binom{n+k}{k}=\binom{n+k-1}{k}+\binom{n+k-1}{k-1}$$

holds. This implies that

$$\binom{n+k}{k}=\binom{n+k-1}{k}+\binom{n+k-2}{k-1}+\ldots+\binom{n}{1}+\binom{n}{0}.$$

Consequently,

$$F_{n+1,k}=\binom{n+k}{k},$$

which shows that the formula $F_{n,k}=\binom{n+k-1}{k}$ for $k = 1, 2, \ldots$ is true for any n.

Another proof of the same formula is this. To each decomposition $k = a_1 + a_2 + \ldots + a_n$ of a natural number k into the sum of n non-negative integers we relate the sequence of the numbers $l_i = a_1 + a_2 + \ldots + a_i + i$, where $i = 1, 2, \ldots, n-1$. It is clear that this sequence consists of increasing natural numbers each of which is $\leqslant n+k-1$. As is known the number of such sequences is equal to $\binom{n+k-1}{n-1}=\binom{n+k-1}{k}$.

T. Skolem [3] has discussed the problem which are the natural numbers n such that the set of the numbers $1, 2, \ldots, 2n$ can be divided into n pairs $(a_i, b_i)(i = 1, 2, \ldots, n)$ in such a way that $b_i - a_i = i$ for any $i = 1, 2, \ldots, n$.

If a number n has this property, then

$$\sum_{i=1}^{n} b_i - \sum_{i=1}^{n} a_i = 1+2+\ldots+n = n(n+1)/2.$$

But, since the numbers $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$ are equal to the numbers $1, 2, \ldots, 2n$ in a certain order, we see that $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = 1+2+\ldots+2n = n(2n+1)$. Hence $\sum_{i=1}^{n} b_i = \frac{1}{4}n(5n+3)$, which is easily proved not to be an integer provided n is congruent to 2 or 3 (mod 4). Conversely, as proved by T. Skolem in the paper referred to above (cf. O'Keefe [1]), if n is congruent to 0 or to 1 (mod 4), then the partition in question is always possible. For example, if $n = 4$, then the pairs of the partition are (6, 7), (1, 3), (2, 5), (4, 8); if $n = 5$, the pairs of the partition are (2, 3), (6,8), (7, 10), (1, 5), (4, 9).

3. Magic squares

A square array of the integers $1, 2, \ldots, n^2$ such that the sums of the numbers in each row, each column and each diagonal are the same is called a *magic square* of degree n. It is easy to calculate that the common value of all these sums is $\frac{1}{2}n(n^2+1)$. The case of $n = 1$ is trivial. For $n = 2$ it is easy to prove that no magic square exists. For $n = 3$ an example of a magic square is

8	1	6
3.	5	7
4	9	2

If $n = 4$, examples of magic squares are the following:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

10	5	11	8
3	16	2	13
6	9	7	12
15	4	14	1

1	15	10	8
14	4	5	11
7	9	16	2
12	6	3	13

4	10	15	5
7	13	12	2
14	8	1	11
9	3	6	16

14	1	12	7
11	8	13	2
5	10	3	16
4	15	6	2

2	13	8	11
12	7	14	1
15	4	9	6
5	10	3	16

Here are the examples for $n = 5, 6, 7$

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	8	25	2	9

1	35	4	33	32	6
25	11	9	28	8	30
24	14	18	16	17	22
13	23	19	21	20	15
12	26	27	10	29	7
36	2	34	3	5	31

30	39	48	1	10	19	28
38	47	7	9	18	27	29
46	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

There exists precisely one magic square for $n = 3$, provided we identify the magic squares obtained from a given one by rotation or reflexion. According to Frenicle, however, there exist 880 magic squares for $n = 4$. It is proved that there exist magic squares for any $n \geqslant 3$ (cf. L. Bieberbach [1]).

The proof of the existence of magic squares for an arbitrarily large n which we are going to present here is due to A. Mąkowski [8]. First we show how, having two magic squares Q_n and Q_m of degree n and m respectively, we can obtain a magic square Q_{nm} of degree nm. This can be done simply by substituting the square Q_n for each number i of the square Q_m provided the number $n^2(i-1)$ is added to each number of the square Q_n. It is easy to see that the square thus obtained is indeed a magic square of degree mn, the sums of the numbers of each column, each row and each diagonal of the square Q_{nm} being equal to $\frac{1}{2}mn(n^2+1)+\frac{1}{2}n^3m(m^2-1)$.

This provides a method of constructing magic squares of degree 3^k, $k = 1, 2, \ldots$, from the magic square of degree 3.

A magic square of an odd degree is called *perfect* if the sum of any two numbers of the square that are in symmetric positions with respect to the number in the middle of the square is equal to double the number in the middle. Any magic square of degree 3 is perfect (the number in the middle being equal to 5). However, there are magic squares of degree five that are not perfect (for example, such is the magic square of degree 5 due to Stifel and presented below). Here is an example of a perfect magic square of degree 5.

11	4	17	10	23
24	12	5	18	6
7	25	13	1	19
20	8	21	14	2
3	16	9	22	15

The magic square of degree seven presented above is perfect.

There exist magic squares that consist of different n^2 integers but not necessarily of the integers $1, 2, \ldots, n^2$. For example,

18	2	13
6	11	16
9	20	4

43	1	67
61	37	13
7	73	31

17	13	2	8
1	9	16	14
18	12	3	7
4	6	19	1

Another more general example is this:

$s-3$	1	$s-6$	8
$s-7$	9	$s-4$	2
6	$s-8$	3	$s-1$
4	$s-2$	7	$s-9$

where $s > 18$.

Magic squares (in the wider sense) have been found consisting of different prime numbers. For example,

569	59	449
239	359	479
269	659	149

17	317	397	67
307	157	107	227
127	277	257	137
347	47	37	367

(cf. Moessner [2] and [3]).

As has been noticed by A. Mąkowski, if the terms of the arithmetical progression $a+b$, $2a+b, \ldots, n^2a+b$ are prime numbers, then replacing the number i by the number $ia+b$ in a magic square consisting of the numbers $1, 2, \ldots, n^2$ we obtain a magic square (in the wider sense) that consists of prime numbers.

As we have already learned, Conjecture H implies the existence of numbers x such that any of the numbers $x+1$, $2x+1, \ldots, n^2x+1$ is prime. Therefore Conjecture H implies the existence of magic squares of degree n for any $n > 2$ consisting of prime numbers.

A. Moessner has constructed a magic square of degree 8 that consists of triangular numbers $t_0, \ldots, t_{63}$. The square is such that the sum of the numbers in each row, each column and each diagonal is the triangular number t_{104}. (Cf. Moessner [1]).

A magic square (in the wider sense) is called *almost magic* if it is formed of the numbers $s, s+1, \ldots, s+n^2$. It is clear that such a square will become a magic square (in the narrower sense) if from any of its numbers the number $s-1$ is subtracted. As announced by L. Bieberbach [1], in the year 1544 Michael Stifel considered almost magic squares which after removing the first and the last row and the first and the last column remain almost magic squares. It can be proved that there exist such squares with an arbitrary > 4 number of rows.

Here is an example of such a square due to Stifel

5	6	23	24	7
22	12	17	10	4
18	11	13	15	8
1	16	9	14	25
19	20	3	2	21

This is a magic square (in the narrower sense) formed of the numbers 1, 2, ..., 25. After removing the first and the last row and the first and the last column of the square we obtain an almost magic square formed of the numbers 9, 10, ..., 17.

The squares formed of natural numbers such that the products of the numbers of each row, each column and each diagonal are the same have also be considered. Such are for instance the squares (cf. Goodstein [1]):

2	256	8
64	16	4
32	1	128

6	36	8
16	12	9
18	4	24

24	81	24
36	36	36
54	16	54

The bibliography concerning magic squares up to the beginning of the 20th century is to be found in P. Bachmann [1]. Many methods of constructions of magic squares are presented in Postnikov [1].

4. Schur's theorem and its corollaries

LEMMA. *If k is a natural number, $N = [ek!]$, if $a_0 < a_1 < a_2 < \dots < a_N$ is a sequence of integers and if the set of the differences $a_j - a_i$, where $0 \leqslant i < j \leqslant N$, is divided into k disjoint classes, then at least one of the classes contains the differences $a_m - a_l$, $a_n - a_l$, $a_n - a_m$ for some l, m, n such that $0 \leqslant l < m < n \leqslant N$.*

PROOF. Suppose to the contrary that for a natural number k the lemma is false. Let K_1 denote the class that contains the maximal possible number of differences of the form $a_j - a_0$, where $0 < j \leqslant N$, and let $a_{j_1} - a_0$, $a_{j_2} - a_0, \dots, a_{j_{k_1}} - a_0$ be the members of the class K_1 ordered according to their magnitude. We then have $N \leqslant k_1 k$.

By assumption, the $k_1 - 1$ differences

$$(1) \qquad a_{j_2} - a_{j_1}, \quad a_{j_3} - a_{j_1}, \quad \dots, \quad a_{j_{k_1}} - a_{j_1}$$

do not belong to the class K_1. Consequently, they must belong to the remaining $k-1$ classes. Let K_2 denote the one that contains the maximal number k_2 of the differences of (1). Suppose that K_2 contains the differences

$$(2) \qquad a_{j_\alpha} - a_{j_1}, \quad a_{j_\beta} - a_{j_1}, \quad a_{j_\gamma} - a_{j_1}, \dots,$$

where $\alpha < \beta < \gamma < \dots$ It is clear that $k_1 - 1 \leqslant k_2 (k-1)$.

If the first number of (2) is subtracted from any of the remaining $k_2 - 1$ numbers, then we obtain the differences

$$(3) \qquad a_{j_\beta} - a_{j_\alpha}, \quad a_{j_\gamma} - a_{j_\alpha}, \quad \dots,$$

which can belong neither to the class K_1 nor to the class K_2. Consequently, they must belong to the remaining $k-2$ classes. Let K_3 denote the class that contains the maximal number k_3 of the numbers of (3). We then have $k_2 - 1 \leqslant k_3 (k-2)$. Continuing in this way we ultimately obtain a sequence of natural numbers $k_1, k_2, \dots, k_s$, where $s \leqslant k$ and

$$(4) \qquad k_i - 1 \leqslant k_{i+1} (k-i) \quad \text{for} \quad i = 1, 2, \dots, s-1,$$

with $k_s = 1$, since, if $k_s > 1$, the procedure described above applied once more would produce the number k_{s+1}. By (4), we infer that

$$\frac{k_i}{(k-i)!} \leqslant \frac{k_{i+1}}{(k-i-1)!} + \frac{1}{(k-i)!}, \qquad i = 1, 2, \dots, s-1,$$

whence, adding the inequalites, we obtain

$$\frac{k_1}{(k-1)!} \leqslant \frac{1}{(k-1)!} + \frac{1}{(k-2)!} + \ldots + \frac{1}{(k-s)!} < e - \frac{1}{k!}.$$

Hence $N \leqslant k_1 k < ek! - 1$, contrary to the definition of N. The lemma is thus proved. □

THEOREM 1 (I. SCHUR (¹)). *Suppose that for a natural number k the numbers $1, 2, \ldots, [ek!]$ are divided into k classes. Then at least one of the classes contains two numbers of the sequence and their difference.*

PROOF. If we set $a_i = i$, $i = 1, 2, \ldots, [ek!]$, in the lemma and note that among the numbers $1, 2, \ldots, [ek!]$ all the differences $a_j - a_i$ with $0 \leqslant i < j \leqslant [ek!]$ appear and, moreover, $a_n - a_m = (a_n - a_1) - (a_m - a_1)$, Theorem 1 follows at once. □

In connection with Theorem 1 one may ask the following question. Given a natural number k, which is the least number $N = N(k)$ which has the same property as the number $[ek!]$, i.e. is such that, if the set of the numbers $1, 2, \ldots, N$ is divided into k classes, then at least one of the classes contains two numbers of the set $1, 2, \ldots, N$ together with their difference. Theorem 1 states that $N(k) \leqslant [ek!]$. Therefore $N(1) \leqslant 2$, $N(2) \leqslant 5$, $N(3) \leqslant 16$. On the other hand, clearly, $N(1) \neq 1$, so $N(1) = 2$. Since the numbers 1, 2, 3, 4 can be divided into two classes, 1, 4 and 2, 3, neither of which contains two numbers together with their difference, we see that $N(2) > 4$; so since $N(2) \leqslant 5$, we have $N(2) = 5$. As proved by I. Schur, $N(k+1) \geqslant 3N(k) - 1$ (cf. Exercise 1, below). Hence $N(k) \geqslant (3^k + 1)/2$, the equality being possible only in the case of $k = 1, 2, 3$.

L. D. Baumert [1] has verified that $N(4) = 45$. Recently Schur's estimates have been improved. From E. G. Whitehead [1] it follows that

$$N(k) \leqslant \left[k!\left(e - \frac{1}{24}\right)\right],$$

while H. L. Abbott and D. Hanson [1] have proved that

$$N(n+m) \geqslant (2N(m) - 1)\, N(n) - N(m) + 1. \tag{5}$$

Since, as was shown by H. Fredericksen [1], $N(5) \geqslant 158$, it follows from inequality (5) with $m = 5$ that

$$N(k) \geqslant 1 + 315^{(k-1)/5}, \quad k = 1, 2, 3, \ldots \tag{6}$$

(¹) Schur [1], cf. also LeVeque [2], vol. 1, p. 60.

THEOREM 2. *Let* $0 < a_0 < a_1 < \ldots < a_N$ *be a sequence of integers with* $N = [ek!]$. *If the sequence contains no arithmetical progression of at least three terms, then any partition of the set* $1, 2, \ldots, a_N$ *into k classes has the following property: at least one of the classes contains two different numbers and their sum.*

The proof is easily deduced from the lemma and from the following three obvious remarks:

1) among the numbers $1, 2, \ldots, a_N$ all the differences $a_j - a_i$ with $0 \leqslant i < j \leqslant N$ are contained,

2) $a_n - a_l = (a_n - a_m) + (a_m - a_l)$,

3) $a_n - a_m \neq a_m - a_l$, since the numbers a_l, a_m, a_n are not in an arithmetical progression.

COROLLARY 1. *If k is a natural number,* $n \geqslant 2^{[ek!]}$, *and the set* $1, 2, \ldots, n$ *is divided into k classes, then at least one of the classes contains two different numbers and their sum.*

To prove the corollary it is sufficient to set $a_i = 2^i$, $i = 0, 1, 2, \ldots, [ek!]$ in Theorem 2 and to note that the sequence 2^i $(i = 0, 1, 2, \ldots)$ does not contain any arithmetical progression that has three terms.

As an immediate consequence of Corollary 1 we have

COROLLARY 2. *If the set of all natural numbers is divided into finitely many classes, then at least one of the classes contains two different natural numbers and their sum* (cf. Rado [1]).

Corollary 1 has been greatly improved by R. W. Irving [1], who has proved that $2^{[ek!]}$ can be replaced by

$$\left[\frac{1}{2} ek! (2k+1)\right] + 2.$$

In connection with Theorem 2 the following question arises. Given a natural number k, which is the least natural number $n = n(k)$ with the following property: if the numbers $1, 2, \ldots, n$ are divided into k classes, then at least one class contains two different numbers together with their sum.

Clearly, we have $n(1) = 3$. It can be proved that $n(2) = 9$. The inequality $n(2) \geqslant 9$ follows from the fact that the set of the numbers $1, 2, \ldots, 8$ can be divided into the classes $A = \{1, 2, 4, 8\}$ and B

$= \{3, 5, 6, 7\}$ such that neither of them contains the sum of any two numbers contained in it. Consequently, in order to prove that indeed $n(2) = 9$, it is sufficient to prove that if the set of the numbers $1, 2, \ldots, 9$ is divided into two classes, then at least one of them is such that it contains two different numbers and their sum. The proof of this fact is presented in detail in my book in Polish (Sierpiński [26], pp. 427–428).

As regards the number $n(3)$, we mention here, that $n(3) \geqslant 24$. The argument follows from the fact that the natural numbers $1, 2, \ldots, 23$ can be divided into three classes A, B, C such that none of the classes contains the sum of any two elements containend in it. In fact, we set $A = \{1, 2, 4, 8, 11, 22\}$, $B = \{3, 5, 6, 7, 19, 21, 23\}$, $C = \{9, 10, 12, 13, 14, 15, 16, 17, 18, 20\}$. On the other hand G. W. Walker [1] has announced (without a proof) that $n(3) = 24$, $n(4) = 67$, $n(5) = 197$. He also formulated the inequality $2n(k) < n(k+1) \leqslant 3n(k)$ for any $k = 1, 2, \ldots$ One part of it is proved in Exercise 2 below, the other is false as a consequence of inequality (6) above.

Another problem connected with this topic is this: Given a natural number N, which is the maximal number $r = r(N)$ such that there exists a sequence $a_1, a_2, \ldots, a_r$ consisting of natural numbers $\leqslant N$ and containing no arithmetical progression that has three terms. (The sequence $a_1, a_2, \ldots, a_r$ is called A-sequence belonging to N.) It is easy to prove that $r(1) = 1$, $r(2) = r(3) = 2$, $r(4) = 3$, $r(5) = r(6) = r(7) = 4$. P. Erdös and P. Turân [1] have proved that $r(8) = 4$, $r(9) = r(10) = 5$, $r(11) = r(12) = 6$, $r(13) = 7$, $r(14) = r(15) = r(16) = r(17) = r(18) = r(19) = 8$, $r(21) = r(22) = r(23) = 9$ (¹) and quoted the conjecture of G. Szekeres that the equality $r(\frac{1}{2}(3^k+1)) = 2^k$ holds for any $k = 0, 1, 2, \ldots$ The conjecture, however, turned out to be false; as is shown by F. Behrend [1], $r(N) > N^{1-c/\sqrt{\log N}}$, where c is a constant (cf. Salem and Spencer [1], [2], Moser [3]).

S. S. Wagstaff, Jr. [1] has computed the values of $r(n)$ for $n \leqslant 53$, finding that $r(24) = r(25) = 10$, $r(26) = \ldots = r(29) = 11$, $r(30) = r(31) = 12$, $r(32) = \ldots = r(35) = 13$, $r(36) = \ldots = r(39) = 14$, $r(40) = 15$, $r(41) = \ldots = r(50) = 16$, $r(51) = r(52) = r(53) = 17$.

On the other hand, K. F. Roth [1] has proved that for a suitable C

$$r(n) < C\frac{n}{\log\log n}, \qquad \text{hence} \qquad \lim_{n\to\infty}\frac{r(n)}{n} = 0.$$

(¹) P. Erdös and P. Turân have stated that $r(20) = 8$ this, however, is not true, because, as shown by A. Mąkowski [2], $r(20) = 9$.

The latter result of Roth and the result of Behrend have been extended to sequences containing no arithmetical progression of k terms by Szemeredi [1] and R.A. Rankin [1], respectively.

EXERCISES. 1. Prove the theorem of I. Schur stating that $N(k+1) \geqslant 3N(k)-1$.

Proof. It follows from the definition of $N(k)$ that the set of the numbers $1, 2, \ldots, N(k)-1$ can be divided into k classes in such a way that none of the classes contains the difference of any two numbers contained in it. Let $K_i = \{x_1^{(i)}, x_2^{(i)}, \ldots, x_{s_i}^{(i)}\}$ $(i = 1, 2, \ldots, k)$. Let

$$L_i = \{3x_1^{(1)}-1, 3x_1^{(i)}-1, 3x_2^{(i)}, \ldots, 3x_{s_i}^{(i)}, 1, 3x_{s_i}^{(i)}\}, \; i = 1, 2, \ldots, k,$$

$$L_{k+1} = \{1, 4, 7, \ldots, 3N(k)-2\}.$$

It is easy to verify that none of the classes L_i $(i = 1, 2, \ldots, k+1)$ contains the difference of any two numbers contained in it and all the classes L_i $(i = 1, 2, \ldots, k+1)$ together contain all the natural numbers $1, 2, \ldots, 3N(k)-2$. It follows from the definition of $N(k+1)$ that $N(k+1) > 3N(k)-2$, whence $N(k+1) \geqslant 3N(k)-1$.

2. Prove that $n(k+1) \geqslant 2n(k)+1$.

PROOF. It follows from the definition of $n(k)$ that the numbers $1, 2, \ldots, n(k)-1$ can be divided into k classes in such a way that none of them contains the sum of any two numbers contained in it. To this classes we add another class consisting of the numbers $n(k), n(k)+1, n(k)+2, \ldots, 2n(k)$. Thus we obtain a partition of the set of the numbers $1, 2, \ldots, 2n(k)$ into $k+1$ classes which has an analogous property. It follows from the definition of the number $n(k+1)$ that $n(k+1) \geqslant 2n(k)+1$. □

REMARK. A. Mąkowski [3] has proved a stronger inequality, namely $n(k+1) \geqslant 2n(k) + \frac{1}{2}k(k+1)+1$.

3. Prove that $r(m+n) \leqslant r(m)+r(n)$ (Erdös and Turán).

The proof follows from the remark that, if $a_1 < a_2 < \ldots < a_r$ is an A-sequence that belongs to the number N, then $a_1-k, \ldots, a_r-k$ is also an A-sequence of N for any $k < a_1$.

4. Prove that $r(2n) \leqslant n$ for $n \geqslant 8$ (Erdös and Turán).

This is proved by induction on n and it follows from the formulae $r(2\cdot 8) = 8$, $r(2\cdot 9) < 9$, $r(2\cdot 10) < 10$, $r(2\cdot 11) < 11$ and from the implication: if $r(2n) \leqslant n$, then $r(2(n+4)) = r(2n+8) \leqslant r(2n)+r(8) \leqslant n+4$.

5. Prove that if $n \geqslant m$, then $r(2n+m-1) \geqslant r(m)+r(n)$.

This follows from the fact that if $a_1 < a_2 \ldots < a_{r(n)}$ is an A-sequence that belongs to n and $b_1 < b_2 < \ldots < b_{r(m)}$ is an A-sequence that belongs to m, then, for $n \geqslant m$, $a_1 < a_2 < \ldots < a_{r(n)} < 2a_{r(n)}+b_1-1 < 2a_{r(n)}+b_2-1 < \ldots < a_{r(n)} < 2a_{r(n)}+b_{r(m)}-1$ is an A-sequence of the number $2n+m-1$ that consists of $r(n)+r(m)$ terms.

6. Prove that $r(\frac{1}{2}(3^k+1)) \geqslant 2^k$ (Erdös and Turán).

The proof is by induction and it follows from the formula $r(\frac{1}{2}(3^0+1)) = r(1)-1 = 2^0$ and from the fact that if $r(\frac{1}{2}(3^k+1)) \geqslant 2^k$, then, by Exercise 5,

$$\begin{aligned} r(\tfrac{1}{2}(3^{k+1}+1)) &= r(2(\tfrac{1}{2}(3^k+1))+\tfrac{1}{2}(3^k+1)-1) \\ &\geqslant r(\tfrac{1}{2}(3^k+1))+r(\tfrac{1}{2}(3^k+1)) \geqslant 2^{k+1}. \end{aligned}$$

7. Prove that $r(51) \geqslant 17$.

The proof follows immediately from the fact (noticed by S. Masłowski) that the sequence 1, 2, 5, 6, 12, 14, 15, 17, 21, 35, 38, 39, 42, 44, 47, 48, 51 does not contain any three numbers in an arithmetical progression.

M. Hall Jr. [2] has proved the existence of a set Z of different natural numbers such that any natural number is the difference of precisely one pair of numbers of the set Z. We are going to construct an infinite sequence of natural numbers that form a set Z which has the required property (cf. Browkin [2]).

Let $a_1 = 1$, $a_2 = 2$. Further, let n denote a natural number and suppose that the numbers $a_1, a_2, \ldots, a_{2n}$ are already defined. We set $a_{2n+1} = 2a_{2n}$.

Now let r_n be the least natural number which cannot be represented in the form $a_j - a_i$ with $1 \leqslant i < j \leqslant 2n+1$. We define a_{2n+2} as $a_{2n+1} + r_n$. We see that the sequence $a_1, a_2, \ldots$ is now well defined by induction. The initial seven terms of the sequence are 1, 2, 4, 8, 16, 21, 42.

It follows from definition of r_n that each of the numbers $1, 2, \ldots, r_n$ is of the form $a_j - a_i$ with $1 \leqslant i < j \leqslant 2n+2$. Hence it follows that $r_{n+1} > r_n$ for any $n = 1, 2, \ldots$ Therefore any natural number can be represented in the form $a_j - a_i$ provided the indices i, j are suitably chosen.

In order to complete the proof that the set Z indeed has the required property, it remains to show that for any natural numbers h, k, l, m with $h < k$ and $l < m$, $k < m$ the inequality $a_k - a_h \neq a_m - a_l$ is valid. Suppose to the contrary that $a_k - a_h = a_m - a_l$. Since $m > k > h \geqslant 1$, we must have $m \geqslant 3$. If m is odd, i.e. $m = 2n+1$, where n is a natural number, then $a_{2n+1} < a_l + a_k \leqslant 2a_{m-1} = 2a_{2n} = a_{2n+1}$, which is impossible. If m is even, i.e. $m = 2n+2$, where n is a natural number, then, in the case of $l = 2n+1$, we have $a_m - a_l = a_{2n+2} - a_{2n+1} = r_n$, which, in virtue of the equality $a_k - a_h = a_m - a_l$, gives $r_n = a_k - a_h$, where $h < k \leqslant m - 1 = 2n + 1$, contrary to the definition of the number r_n. In the case of $l < 2n+1$ (which in virtue of $l < m$ is the only possibility provided $l = 2n+1$ is excluded) for $k = 2n+1$, we have $a_m - a_k = a_l - a_h$, whence, since $k < m$, we have $h < l \leqslant 2n$ and $a_m - a_k = a_{2n+2} - a_{2n+1} = r_n$; so $r_n = a_l - a_h$ with $h < l \leqslant 2n$, contrary to the definition of r_n. Finally, if $l < 2n+1$ and $k < 2n+1$, then $a_{2n+2} = a_m = a_l + a_k - a_h < a_l + a_k < a_{2n} + a_{2n} = a_{2n+1}$, which is impossible.

Thus we see that the sequence $a_1, a_2, \ldots$ has the required property.

It will be observed that if the axiom of choice is assumed, a similar property can be proved for real numbers. One can prove the existence of a set X consisting of real numbers and such that any positive real number is uniquely expressible as the difference of two numbers of the set X(¹).

5. Odd numbers which are not of the form 2^k+p, where p is a prime

In the year 1849 A. de Polignac [1] formulated the conjecture that any odd number $n > 1$ is of the form 2^k+p, where k is a natural number and p is either a prime or the number 1. In 1950 P. Erdös [10] proved that there exist infinitely many odd numbers for which the conjecture fails (cf. also van de Corput [3]).

THEOREM 3 (Erdös [10]). *There exists an infinite arithmetical progression of odd numbers none of which is of the form* 2^k+p, *where* $k = 0, 1, 2, \ldots$, *and* p *is a prime.*

LEMMA. *Every natural number satisfies at least one of the following six congruences:*

$$(1)\ k \equiv 0 \pmod 2,\quad (2)\ k \equiv 0 \pmod 3,\quad (3)\ k \equiv 1 \pmod 4,$$

$$(4)\ k \equiv 3 \pmod 8,\quad (5)\ k \equiv 7 \pmod{12},\quad (6)\ k \equiv 23 \pmod{24}.$$

PROOF OF THE LEMMA. If a number k does not satisfy (1) or (2), then it is divisible neither by 2 nor by 3 and thus it must be of the form $24t+r$, where t is an integer and r is one of the numbers 1, 5, 7, 11, 13, 17, 19, 23. But a straightforward verification shows that then k must satisfy congruences (3), (3), (5), (4), (3), (3), (4), (6), respectively. □

COROLLARY. *If k is a non-negative integer, then at least one of the following congruences holds:*

$$(7)\ 2^k \equiv 1 \pmod 3,\qquad (8)\ 2^k \equiv 1 \pmod 7,$$

$$(9)\ 2^k \equiv 2 \pmod 5,\qquad (10)\ 2^k \equiv 2^3 \pmod{17},$$

$$(11)\ 2^k \equiv 2^7 \pmod{13},\quad (12)\ 2^k \equiv 2^{23} \pmod{241}.$$

(¹) Cf. Piccard [1], pp. 36–37 (Remarque), and Lindenbaum [1], p. 25, Corollaire 17, and footnote (27) on page 24.

Proof of the Corollary. We simply verify that $2^2 \equiv 1 \pmod 3$, $2^3 \equiv 1 \pmod 7$, $2^4 \equiv 1 \pmod 5$, $2^8 \equiv 1 \pmod{17}$, $2^{12} \equiv 1 \pmod{13}$, $2^{12} \equiv -1 \pmod{241}$, whence $2^{24} \equiv 1 \pmod{241}$. From this we infer that the congruences (1), (2), (3), (4), (5), (6) imply the congruences (7), (8), (9), (10), (11), (12), respectively. □

Proof of the Theorem. In virtue of the Chinese remainder theorem there exists a natural number a that satisfies the congruences $a \equiv 1 \pmod 2$, $a \equiv 1 \pmod 3$, $a \equiv 1 \pmod 7$, $a \equiv 2 \pmod 5$, $a \equiv 2^3 \pmod{17}$, $a \equiv 2^7 \pmod{13}$, $a \equiv 2^{23} \pmod{241}$, $a \equiv 3 \pmod{31}$ and, moreover, there exists an infinite arithmetical progression of a's each of which satisfies these congruences. Clearly, the terms of the arithmetical progression must be odd. If a is any term of the arithmetical progression, then, since it satisfies the congruences, the corollary of the lemma implies that the number $a-2^k$ is divisible by at least one of the primes 3, 7, 5, 17, 13, 241. On the other hand, $a \equiv 3 \pmod{31}$ and for any $k = 1, 2, \ldots$ the number 2^k is congruent to one of the numbers 1, 2, 4, 8, 16 (mod 31) (this is because $2^5 \equiv 1 \pmod{31}$). Consequently, $a-2^k$ is congruent to one of the numbers 2, 1, -1, -5, -13 (mod 31). But none of these numbers is congruent (mod 31) to any of the numbers 3, 7, 5, 17, 13, 241. Therefore the number $a-2^k$ cannot possibly be any of these numbers, but, on the other hand, it is divisible by at least one of them. Therefore it is a composite number. Hence it follows that the number $a-2^k$ cannot be a prime for any non-negative integer k; consequently, a cannot be of the form $a = 2^k+p$, where $k = 0, 1, 2, \ldots$, and p is a prime. Thus we see that the terms of the arithmetical progression which we have defined above have the required property. This proves the truth of Theorem 3. □

The proof of Theorem 3 shows that there exist infinitely many natural numbers n such that for any non-negative integer k the number $-n-2^k$ and thus also the number $n+2^k$ are divisible by at least one of the numbers 3, 7, 5, 17, 13, 241. Let P denote the product of these primes. In virtue of what we proved above the number $n+2^{k[\varphi(P)-1]}$ has a prime divisor $p \mid P$. But $2^{k\varphi(P)} \equiv 1 \pmod P$, which in virtue of $n+2^{k[\varphi(P)-1]} \equiv 0 \pmod p$ gives $n \cdot 2^k+1 \equiv 0 \pmod p$, which for n large enough (e.g. for $n > 241$) gives a composite number $n \cdot 2^k+1$. Thus we have proved the following

Corollary. *There exist infinitely many natural numbers n such that each of* *the numbers* $n \cdot 2^k+1$, *where* $k = 0, 1, 2, \ldots$, *is composite* (cf. Sierpiński [28] and Chapter X, § 4, Ex. 3).

THEOREM 4 (R. Crocker). *There exist infinitely many natural numbers that are not representable as sums of two different powers of* 2 (*with non-negative exponents*) *and a prime number.*

PROOF. We are going to show that the numbers that have the required property are the numbers $2^{2^n}-1$, $n = 3, 4, \ldots$ In fact, suppose that for a natural number $n > 2$ we have $2^{2^n}-1 = 2^k+2^l+p$, where k, l are integers and $k > l \geqslant 0$. We note that the equality $l = 0$ is impossible, because otherwise we would have $p = 2^{2^n}-2^k-2 = 2(2^{2^n-1}-2^{k-1}-1)$ and, since $2^n > k$, $k-1 \leqslant 2^n-2$, whence $2^{2^n-1}-2^{k-1} \geqslant 2^{2^n-1}-2^{2^n-2} = 2^{2^n-2} \geqslant 2^{2^3-2} = 2^6$, and thus $2^{2^n-1}-2^{k-1}-1 \geqslant 2^6-1 > 1$, which is impossible since p is a prime. Consequently, we have $l \geqslant 1$, and so $k > 1$. Let h denote the greatest non-negative exponent for which 2^h divides $k-l$. The number $(k-l)/2^h$ is then odd and $2^{2^h}+1 \mid 2^{k-l}+1$. Since $p = 2^{2^n}-2^k-2^l-1 = 2^{2^n}-1-2^l(2^{k-l}+1)$, the divisibility relations obtained above give $2^{2^h}+1 \mid p$, whence, in virtue of the fact that p is a prime, we infer that $p = 2^{2^h}+1$. Consequently, $2^{2^n} = 2^k+2^l+2^{2^h}+2$. Since $2^n > k > 1$, the number $2^l+2^{2^h}+2$ is divisible by 4. Therefore either $l = 1$ or $2^h = 1$. If $2^h = 1$, then $l > 1$ and so $2^{2^n-2} = 2^{k-2}+2^{l-2}+1$, which is impossible because the left-hand side of the equality is divisible by 2^6. Thus, necessarily, $l = 1$, $2^h > 1$, whence $2^{2^n-2} = 2^{k-2}+2^{2^h-2}+1$, which (in virtue of $2^n-2 \geqslant 6$) proves that precisely one of the two possible cases $k = 2$ and $2^h = 2$ can occur. If $k = 2$, then $2^h \mid k-l = 1$, which is impossible because $2^h > 1$. If $2^h = 2$, then $k \geqslant 3$ and $2^{2^n-3} = 2^{k-3}+1$, which, in virtue of $n \geqslant 3$, gives $k = 3$, and so $n = 2$, which again is impossible.

This completes the proof of the fact that the numbers $2^{2^n}-1$ have the required property. □

COROLLARY (Crocker [1]). *None of the numbers* $2^{2^n}-5$, *where* $n = 3, 4, 5, \ldots$, *is of the form* 2^k+p, *where* $k = 0, 1, 2, \ldots$ *and* p *is a prime.*

PROOF OF THE COROLLARY. If $2^{2^n}-5 = 2^k+p$, where k is a non-negative integer and p is a prime, then $2^{2^n}-1 = 2^k+2^2+p$, whence, in view of $n \geqslant 3$, the fact that the numbers $2^{2^n}-1$ have the property just shown implies that k must be equal to 2; consequently $2^{2^n}-1 = 2^3+p$, and so

$p = 2^{2^n} - 9 = (2^{2^n-1} - 3)(2^{2^n+1} + 3)$, whence $2^{2^n-1} - 3 = 1$, contrary to the assumption that $n \geqslant 3$. □

By an ingenious refinement of the argument used in the proof of Theorem 4, R. Crocker [2] proved the existence of infinitely many odd natural numbers that are not representable as sums of two powers of 2 (different or not) and a prime number.

CHAPTER XIII

COMPLEX INTEGERS

1. Complex integers and their norm. Associated integers

The *complex* or *Gaussian integers* are the complex numbers $a+bi$, where a, b are integers.

The theory of complex integers is important for two reasons, firstly because it is interesting to see how far the properties of ordinary integers are susceptible to generalization, and secondly because various properties of ordinary integers themselves follow most simply from those of the wider class. The proofs of these properties obtained in another way turn out to be much more difficult.

An immediate consequence of the definition of arithmetical operations on complex numbers is that the sum, the difference and the product of two or more complex integers is also a complex integer.

EXERCISES. 1. Find all the possible representations of the number 0 as the sum of the squares of two complex integers.

ANSWER. $0 = (a+bi)^2+(\pm b\mp ai)^2$, where a, b are arbitrary rational integers, and either both upper or both lower signs are taken.

2. Find the complex integers $x+yi$ which are representable as sums of the squares of two complex integers.

SOLUTION. In order that an integer $x+yi$ be the sum of the squares of two complex integers it is necessary and sufficient that y should be even and, in the case where x is of the form $4t+2$, y should be divisible by 4.

The condition is necessary because if

$$x+yi = (a+bi)^2+(c+di)^2,$$

then

$$x = a^2-b^2+c^2-d^2, \qquad y = 2(ab+cd).$$

Hence, as one verifies directly, if x is of the form $4t+2$ at least one of the numbers a and b and at least one of the numbers c and d are even. But then the number $ab+cd$ is even, which shows that y is divisible by 4.

The condition is also sufficient because, if $x = 2t+1$ and $y = 2u$, then

$$x+yi = (t+1+ui)^2+(u-ti)^2.$$

If $x = 4t+2$ and $y = 4u$, then

$$x+yi = (t+u+1+(u-t)i)^2+(t-u+1+(t+u)i)^2.$$

If $x = 4t$ and $y = 4u$, then

$$x+yi = (t+1+ui)^2+(u+(1-t)i)^2,$$

finally, if $x = 4t$ and $y = 4u+2$, then

$$x+yi = (t+u+1+(u+1-t)i)^2+(t-u+(t+u)i)^2.$$

3. Prove that a complex integer $x+yi$ is representable as the sum of the squares of three complex integers if and only if y is even.

HINT. Use Exercise 2 and the identity

$$4t+2+2ui = 4t+1+2ui+1^2.$$

4. Prove that a complex integer $a+bi \neq 0$ is the square of a complex integer if and only if

$$a^2+b^2 = c^2, \quad c+a = 2x^2 \quad \text{and} \quad c-a = 2y^2,$$

where c is a natural number and x, y are rational integers. Prove that then

$$a+bi = (\pm x \pm yi)^2,$$

where the signs should be identical if $b > 0$ and opposite if $b < 0$.

REMARK. The theorem formulated in Exercise 4 may be thought of as a test for verifying whether a given complex number is the square of a complex integer, and as a method of finding the complex integral square roots of a complex integer (in the case where such roots exist).

For a given complex number $z = a+bi$ we denote by z' its conjugate complex number, i.e. the number $z' = a-bi$.

As an immediate consequence of the definition of the arithmetical operations on complex numbers, we have

(1) if $z = t+u$, then $z' = t'+u'$,

(2) if $z = t-u$, then $z' = t'-u'$,

(3) if $z = tu$, then $z' = t'u'$.

Clearly, either the numbers z and z' are both complex integers or none of them is a complex integer. The number $(z')'$, the conjugate of z', is equal to z.

The product zz' of two conjugate numbers is called the *norm* of the number z and denoted by $N(z)$. We write

$$N(z) = zz'.$$

Consequently, if $z = a+bi$ (where a, b are real numbers), we have

$$N(z) = a^2+b^2$$

Therefore the norm of a complex number is always real and non-negative, being equal to zero only if $a = b = 0$, i.e. if $z = 0$.

Moreover, the norm of a non-zero complex integer is a natural number.

The conjugates have the same norm. We say that a complex integer z is *divisible* by a number t if there exists a complex integer u such that

$$z = tu. \tag{4}$$

We then write $t \mid z$.

To establish whether a complex integer $a+bi$ is divisible by a complex number $c+di$, not equal to 0, one has to know whether certain divisibilities among rational integers hold. In fact, the formula

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i$$

implies that

$$c+di \mid a+bi$$

is valid if and only if

$$c^2+d^2 \mid ac+bd \quad \text{and} \quad c^2+d^2 \mid bc-ad.$$

For example,

$$3+5i \mid 21+i \quad \text{because} \quad 34 \mid 68 \quad \text{and} \quad 34 \mid -102,$$

$$1+i \mid 2 \quad \text{because} \quad 2 \mid 2 \quad \text{and} \quad 2 \mid -2;$$

on the other hand,

$$1-2i \nmid 1+2i \quad \text{because} \quad 5 \nmid -3.$$

It follows from (3) that, if $t \mid z$, then $t' \mid z'$ and if $z = tu$, then

$$zz' = tut'u' = tt'uu',$$

whence, by the definition of the norm of a complex number,

$$N(z) = N(t)\,N(u). \tag{5}$$

We express this by saying that the *norm of the product of two complex numbers is the product of their norms.*

This theorem is easily generalized to the product of any finite number of factors.

By (5) we also have $N(t) \mid N(z)$; consequently, *if a complex integer t is a divisor of a number z, then the norm of t is a divisor of the norm of z.*

The converse, however, is not true. For example, $N(1-2i) = N(1+2i)$ but $1-2i \nmid 1+2i$.

Two complex integers, both not 0, which divide each other are called *associated.*

Consequently, z and t are associated if and only if $t \mid z$ and $z \mid t$. We then have $N(t) \mid N(z)$ and $N(z) \mid N(t)$, which, in virtue of the fact that the norm of a non-zero complex integer is different from zero, gives $N(t) = N(z)$.

Thus *any two associated complex integers have equal norms* (the converse is false: the numbers $1-2i$ and $1+2i$ have equal norms but are not associated because, as we have learned, $1-2i \nmid 1+2i$).

Now we are going to find the associates of a given complex integer $z \neq 0$.

Let t be associated with z; then, for a complex integer u, we have $t = zu$, whence

$$N(t) = N(z)N(u). \tag{6}$$

But, since associates have equal norms, $N(z) = N(t)$ and $N(z) \neq 0$ because $z \neq 0$. Consequently, (6) proves that $N(u) = 1$.

Let $u = a+bi$, whence $a^2+b^2 = 1$. Therefore, either $a = \pm 1$ and $b = 0$, or, conversely, $a = 0$ and $b = \pm 1$. From this we conclude that u is one of the four numbers $1, -1, i, -i$, and so $t = zu$ is one of the four numbers

$$z, \quad -z, \quad iz, \quad -iz. \tag{7}$$

Thus we see that any associate of z is one of the numbers (7). Conversely, it is easy to see that each of the numbers (7) is associated with z. This is because $z = (-1)(-z) = (-i)iz = i(-iz)$. Thus we arrive at

THEOREM 1. *Any complex integer z, not equal to 0, has exactly four associates, namely, the numbers* (7).

It is clear that (since $z \neq 0$) all the four associates are different.

In problems concerning divisibility of complex integers, associated numbers can be replaced by one another. The reason is that, if z is divisible by t, then any associate of z is divisible by any associate of t.

It is also clear that if z is associated with t, then z' is associated with t'.

If two complex integers z_1 and z_2 are divisible by t, then their sum and their difference are divisible by t. In fact, if $z_1 = tu$ and $z_2 = tv$, then $z_1 \pm z_2 = t(u \pm v)$.

If a complex integer z is divisible by t and t is divisible by u, then z is divisible by u. In fact, if $z = tw$ and $t = uv$, then $z = uvw$.

This, in consequence, shows that, if t is a common divisor of complex integers $z_1, z_2, \ldots, z_n$ and if $u_1, u_2, \ldots, u_n$ are any complex integers, then $t \mid z_1 u_1 + z_2 u_2 + \ldots + z_n u_n$.

2. Euclidean algorithm and the greatest common divisor of complex integers

We now prove

THEOREM 2. *If z and $t \neq 0$ are complex integers, then there exist complex integers c and r such that*

$$z = ct + r \tag{8}$$

and

$$N(r) \leqslant \tfrac{1}{2} N(t), \tag{9}$$

whence $N(r) < N(t)$.

PROOF. Let

$$z/t = x + yi, \tag{10}$$

where x, y are rationals. Let ξ and η be the integers closest to x and y, respectively. Then we may write

$$x = \xi + x_1, \quad y = \eta + y_1, \tag{11}$$

where x_1 and y_1 are rational numbers such that

$$|x_1| \leqslant \tfrac{1}{2}, \quad |y_1| \leqslant \tfrac{1}{2}, \tag{12}$$

Let

$$c = \xi + \eta i, \quad r = z - ct. \tag{13}$$

It is clear that c, r are complex integers and that they satisfy (8). At the same time, by (10), (11), (13), we have

$$r = z - ct = (x + yi)t - (\xi + \eta i)t = (x_1 + y_1 i)t.$$

Since the norm of a product is equal to the product of the norms of the factors, we obtain by (12)

$$N(r) = N(x_1 + y_1 i) N(t) = (x_1^2 + y_1^2) N(t), \qquad x_1^2 + y_1^2 \leqslant \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}$$

which proves (9) and at the same time completes the proof of the theorem. □

The theorem just proved provides an algorithm similar to the Euclidean algorithm proved for rational integers.

It embodies the ordinary process for finding the greatest common divisor of two given complex integers, z and $t \neq 0$. At first, by means of Theorem 2, we find the numbers c, r. By (8), we infer that the numbers z and t have the same common divisors as the numbers t and r. Moreover, by (5), $N(r) < N(t)$. Thus in order to find the common divisors of the numbers z and t it is sufficient to find the common divisors of the numbers t and r, where $N(r) < N(t)$.

If $r = 0$, then the common divisors of the numbers z and t are precisely the divisors of the number t.

If $r \neq 0$, then we apply the above procedure with the numbers t, r in place of z, t. Thus to find the common divisors of the numbers t, r we have to find the common divisors of the numbers r, r_1, where $N(r_1) < N(r)$.

If $r_1 \neq 0$, we find another number r_2, and so on.

The sequence $r, r_1, r_2, \ldots$ cannot be infinite, because the corresponding sequence of norms is a strictly decreasing sequence of natural numbers. Therefore, for some n, $r_n = 0$. Then the common divisors of r_{n-1} and r_{n-2} are precisely the divisors of the number r_n. Thus we reach the conclusion that there exists a complex integer ϱ whose divisors are precisely the common divisors of the numbers z and t.

This shows that two given complex integers different from zero have at least one common divisor that is divisible by any of their common divisors. It is a natural thing to call it the *greatest common divisor* of the given two complex integers.

Now we are going to establish the number of the greatest common divisors of two complex integers. Let d and δ be the greatest common divisors of complex integers z, t. The numbers d, δ are divisible each by the other, therefore they are associated complex integers. Hence, by Theorem 2, we obtain the following

COROLLARY. *Any two complex integers different from* 0 *have precisely four greatest common divisors, these being associated with each other.*

Actually, rational integers also have two greatest common divisors which differ in the sign. They are such that each of them is divisible by any common divisor of the given numbers. However, if we find the number of common divisors, we do not distinguish between the divisors that differ in the sign only. Similarly, in the case of complex integers we could consider only one greatest common divisor of any two complex integers identifying associated divisors. At any rate, either approach is nothing but a more or less convenient convention.

EXAMPLES. **1.** By means of the algorithm presented above we find the greatest common divisors of the numbers $6-17i$ and $18+i$. Using the successive steps of the algorithm, we find

$$\frac{6-17i}{18+i} = \frac{(6-17i)(18-i)}{18^2+1} = \frac{91-312i}{325} = -i+\frac{91+13i}{325},$$

$$6-17i = -i(18+i)+(5+i),$$

$$\frac{18+i}{5+i} = \frac{(18+i)(5-i)}{5^2+1} = \frac{91-13i}{26} = 3+\frac{1-i}{2},$$

$$18+i = 3(5+i)+3-2i,$$

$$\frac{5+i}{3-2i} = \frac{(5+i)(3+2i)}{3^2+2^2} = 1+i.$$

Therefore the greatest common divisors of the numbers $6-17i$ and $18+i$ are the number $3-2i$ and the numbers associated with it, i.e. $-3+2i$, $2+3i$, $-2-3i$.

2. We find the greatest common divisors of the numbers $2+3i$ and $2-3i$. We have

$$\frac{2+3i}{2-3i} = \frac{(2+3i)^2}{2^2+3^2} - \frac{-5+12i}{13} = i+\frac{-5-i}{13},$$

$$2+3i = i(2-3i)+i-1,$$

$$\frac{2-3i}{i-1} = \frac{-(2-3i)(i+1)}{2} = \frac{-5+i}{2} = -3+\frac{1+i}{2},$$

$$2-3i = -3(i-1)-1.$$

Therefore the greatest common divisors of the numbers $2+3i$ and $2-3i$ are the number 1 and its associates: -1, i and $-i$.

3. We find the greatest common divisors of the numbers $31+i$ and $5+i$. We have

$$\frac{31+i}{5+i} = \frac{(31+i)(5-i)}{5^2+1^2} = \frac{156-26i}{26} = 6-i.$$

Therefore the greatest common divisors of the complex integers $31+i$ and $5+i$ are the number $5+i$ and its associates: $-5-i$, $-1+5i$ and $1-5i$.

It is easy to see that the greatest common divisors have the greatest norm among all the common divisors of the numbers, the converse being also true. So the greatest common divisors could also be defined as the common divisors whose norms assume the greatest possible values. These, however, would make it more difficult to prove the most important property of the greatest common divisors, namely that they are divisible by any common divisor.

The theory of the greatest common divisors of two or more complex integers can easily be established by considering linear forms, just as has been done in the case of rational integers. In fact, let $a_1, a_2, \ldots, a_m$ be complex integers different from zero. Let Z be the set of non-zero numbers of the form

$$a_1 z_1 + a_2 z_2 + \ldots + a_m z_m,$$

where $z_1, z_2, \ldots, z_m$ are complex integers. Finally, let M be the set of the values of the norm of the numbers of Z. Clearly, M is a set of natural numbers. Let n be the least natural number of the set M. Therefore there exists a number ζ in Z such that $N(\zeta) = n$, which means that there exist complex integers $\zeta_1, \zeta_2, \ldots, \zeta_m$ such that

$$(14) \qquad \zeta = a_1 \zeta_1 + a_2 \zeta_2 + \ldots + a_m \zeta_m .$$

We are going to show that each number of the set Z is divisible by ζ. In fact, let z be any number of the set Z. Then there exist complex integers $z_1, z_2, \ldots, z_m$ that

$$(15) \qquad z = a_1 z_1 + a_2 z_2 + \ldots + a_m z_m .$$

Moreover, by Theorem 2, there exist complex integers c and r such that

$$(16) \qquad z = c\zeta + r \quad \text{and} \quad N(r) < N(\zeta).$$

If $r \neq 0$, then r belongs to Z because, by (14), (15) and (12),

$$r = z - c\zeta = a_1 (z_1 - c\zeta_1) + a_2 (z_2 - c\zeta_2) + \ldots + a_m (z_m - c\zeta_m),$$

and, moreover, the numbers $z_j - c\zeta_j$, $j = 1, 2, \ldots, m$, are complex integers. But then, by (16), r is a number whose norm is less than the norm n of ζ, contrary to the definition of n. Consequently $r = 0$, whence, by (16), $z = c\zeta$ and so $\zeta \mid z$.

It is clear that each of the numbers $a_1, a_2, \ldots, a_m$ belongs to the set Z. Therefore, in virtue of what we proved above, the complex integer ζ is a common divisor of the numbers $a_1, a_2, \ldots, a_m$.

Now let δ be any common divisor of these numbers. Then there exist complex integers $t_1, t_2, \ldots, t_m$ such that $a_j = t_j \delta$ for any $j = 1, 2, \ldots, m$. Hence, by (14),

$$\zeta = (t_1 \zeta_1 + t_2 \zeta_2 + \ldots + t_m \zeta_m) \delta,$$

which shows that $\delta \mid \zeta$. From this we conclude that ζ is a common divisor of the numbers $a_1, a_2, \ldots, a_m$ which is such that any common divisor of these numbers divides it. At the same time we have proved that ζ is representable in form (14), where $\zeta_1, \zeta_2, \ldots, \zeta_m$ are complex integers.

Any two complex integers a, b have at least four common divisors, 1, -1, i, $-i$.

If the complex integers a, b have no more than these four divisors, they are called *relatively prime*. We then write $(a, b) = 1$.

It is easy to see that then there exist complex integers x, y which satisfy the equation

$$ax+by = 1. \tag{17}$$

In fact, if $(a, b) = 1$, the number ζ defined by (14) with $a = a_1$, $b = a_2$, $m = 2$ must be one of the numbers 1, -1, i, $-i$. Consequently, one of the numbers ζ, $-\zeta$, $i\zeta$, $-i\zeta$ must be equal to 1 and this implies that for an appropriate choice of complex integers x, y (17) holds.

On the other hand, (17) implies that any common divisor of the numbers a, b, is a divisor of the number 1, therefore the numbers a, b cannot possibly have any common divisor different from 1, -1, i, $-i$, this being equivalent to saying that $(a, b) = 1$.

THEOREM 3. *Two complex integers a, b are relatively prime if and only if there exist complex integers x, y such that $ax+by = 1$.*

Now we consider three complex integers a, b, c, about which we assume that $(a, b) = 1$ and $b \mid ac$. We prove that then $b \mid c$.

In fact, since $(a, b) = 1$, by Theorem 3 there exist complex integers x, y which satisfy equation (17). This, multiplied by c, gives

$$acx+bcy = c. \tag{18}$$

By assumption, $b \mid ac$ and, clearly, $b \mid bc$ for any b. Therefore (18) implies that $b \mid c$, which was to be proved. Thus we have obtained.

THEOREM 4. *For any complex integers a, b, c the relations $(a, b) = 1$ and $b \mid ac$ imply $b \mid c$.*

Another consequence of Theorem 3 is

THEOREM 5. *If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.*

PROOF. If $(a, b) = 1$ and $(a, c) = 1$, then there exist complex integers x, y, u, v such that $ax+by = 1$ and $au+cv = 1$. Multiplying together these equalities we obtain $a(x(au+cv)+buy)+bcyv = 1$, whence $(a, bc) = 1$. □

3. The least common multiple of complex integers

Let $a_1, a_2, \ldots, a_m$ be complex integers different from zero. There are of course non-zero common multiples of these numbers, e.g. the one obtained by multiplying by one another. Among them we select those for which the norm is the least, i.e. not greater than the norm of any common multiple in question. Let v be such a common multiple of $a_1, a_2, \ldots, a_m$. We prove that any common multiple of the numbers $a_1, a_2, \ldots, a_m$ is divisible by v.

In fact, let z be any common multiple of these numbers. By Theorem 2 there exist complex integers c, r such that $z = cv+r$ and $N(r) < N(v)$. If r were not equal to zero, then r, being a common multiple of $a_1, a_2, \ldots, a_m$, would have a norm less than v, contrary to the definition of the number v. Consequently $r = 0$, and this means that there exists at least one common multiple of the numbers $a_1, a_2, \ldots, a_m$ which is such that any common multiple of these numbers is divisible by it.

The norm of any common multiple with this property is, in fact, not greater than the norm of any non-zero common multiple of the numbers $a_1, a_2, \ldots, a_m$. We call it the *least common multiple* of the numbers $a_1, a_2, \ldots, a_m$.

It is easy to see that all the least common multiples of the numbers $a_1, a_2, \ldots, a_m$ are associated and that their norm is the least among the norms of non-zero common multiples of these numbers.

EXERCISE. Find the solution of the equations

$$x+y+z = xyz = 1$$

in complex integers.

SOLUTION. Since $xyz = 1$, the numbers x, y, z must be divisors of unity, i.e. they must be numbers of the sequence $1, -1, i, -i$. Again from $xyz = 1$ it follows that they cannot all be imaginary; on the other hand, the equality $x+y+z = 1$ shows that if the three of them are real, then two are equal to 1, the third being equal to -1, but this contradicts the $xyz = 1$. Therefore at least one of the numbers x, y, z is imaginary, but then, by $x+y+z = 1$, at least two of them are imaginary. Thus we arrive at the final conclusion that one of the numbers x, y, z must be i, the others being $-i$ and 1. We see that the only solutions of our system of equations are $x = 1$, $y = i$, $z = -i$ and those which can be obtained from them by permuting the numbers $1, i, -i$. The number of solutions is thus equal to 6.

REMARK. As is proved by J. W. S. Cassels [4], the system of equations $x+y+z = xyz = 1$ has no solutions in ordinary rational numbers x, y, z (for a simpler proof see Sansone and Cassels [1]).

4. Complex primes

Since any complex integer has at least the four divisors $1, -1, i, -i$ and, moreover, any complex integer z, not an associate of 1, has other four divisors, namely $z, -z, iz, -iz$, we see that any such complex integer has at least eight different divisors.

The complex integers which have precisely the 8 divisors are called *primes*.

In other words, a complex integer is prime if it has no divisors except its associates, and the associates of 1, and moreover, if it is not associated with 1.

It is clear that this definition is equivalent to the following one:

A complex integer is a prime if its norm is greater than 1 and if it is not representable as the product of complex integers with norms greater than 1.

In fact, if ζ is a complex integer, $N(\zeta) > 1$ and $\zeta = \mu\nu$, where $N(\mu) > 1$ and $N(\nu) > 1$, then the number μ cannot be associated either with 1, because, if it could, $N(\mu) = 1$, nor with ζ, because then $N(\mu) = N(\zeta)$, whence, by $N(\zeta) = N(\mu)N(\nu)$, it would follow that $N(\nu) = 1$, contrary to the assumption. Consequently, ζ has a divisor μ which is not associated with 1 or with ζ, and so it is not a prime.

On the other hand, if ζ is a complex integer with $N(\zeta) > 1$ and if it is not a prime, then, by definition, it has a divisor μ which is not associated either with 1 or with ζ. We then have $\zeta = \mu\nu$, where ν is a complex integer.

If $N(\mu) = 1$, then μ is associated with 1, contrary to the assumption (in fact, if for a complex integer $a+bi$ we have $N(a+bi) = 1$, then $a^2+b^2 = 1$, whence, since a, b are rational integers, either $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$).

If $N(\nu) = 1$, then the number ν is associated with 1, whence, by $\zeta = \mu\nu$, the number μ is associated with ζ, contrary to the assumption.

Consequently, $N(\mu) > 1$ and $N(\nu) > 1$, and so the number ζ is the product of two complex integers with norms greater than 1.

It is clear that *any complex integer which is associated or conjugated with a prime complex integer is a prime complex integer.*

THEOREM 6. *Any complex integer whose norm is greater than 1 is representable as the product of finitely many prime complex integers.*

PROOF. Suppose to the contrary that there is a complex integer with a norm n greater than 1 which is not representable as the product of finitely many prime complex numbers. Let M be the set of the values of the norm of all the complex integers with this property. Thus M is a non-void set of natural numbers. Let m be the least number belonging to M. Accordingly, there exists a complex integer z with norm m which is not representable as the product of finitely many prime complex integers. By assumption, z is not a prime and its norm is $m > 1$. Consequently, it is the product of two complex integers, μ and ν, with norms greater than 1. Moreover, $m = N(z) = N(\mu\nu) = N(\mu)N(\nu)$, whence it follows that $N(\mu) < m$ and $N(\nu) < m$. From the definition of m we infer that each of the numbers μ, ν is representable as the product of finitely many prime complex integers. But this shows that also the number $z = \mu\nu$ is representable in such a form, contrary to the definition of z. The theorem is thus proved. □

By definition any prime complex integer π has precisely the eight divisors

$$1, \quad -1, \quad i, \quad -i, \quad \pi, \quad -\pi, \quad i\pi, \quad -i\pi.$$

From this we infer that, *if a complex integer λ is not divisible by a prime complex integer π, then $(\lambda, \pi) = 1$.*

A natural number which is a prime complex integer is of course a prime (in the ordinary sense). The converse, however, is not true: there are primes which are not prime complex integers. For example,

$$2 = (1+i)(1-i) \quad \text{and} \quad N(1+i) = N(1-i) = 2 > 1.$$

The numbers $1+i$ and $1-i$ are prime complex integers. This follows from the fact that, if $1 \pm i = \mu\nu$, then

$$N(\mu)N(\nu) = N(\mu\nu) = N(1 \pm i) = 2;$$

so (in virtue of the fact that the norm of a complex integer is a natural number) we must have $N(\mu) = 1$ or $N(\nu) = 1$, which proves that either μ or ν is associated with 1.

The numbers $1+i$ and $1-i$ are associated because $1-i = -i(1+i)$. Thus we see that the number 2 is associated with the square of a prime complex integer.

Using Theorem 4 one can easily prove that the representation of a complex integer as a product of prime complex integers is unique apart from the order of the primes and ambiguities of associated primes.

In this connection, we are going to characterize the prime complex integers in the set of all complex integers.

We start with determining the natural numbers which, regarded as complex integers, are prime. Clearly, they must be ordinary primes, and, moreover, they should be odd, since the number two has been shown not to be of this sort. Thus we have to consider the primes of the form $4k+1$ and $4k+3$, where k is a natural number.

Let p be a prime of the form $4k+1$. By Theorem 9, Chapter V, there exist natural numbers a, b such that $p = a^2+b^2$, whence $p = (a+bi)(a-bi)$ and, moreover, $N(a \pm bi) = a^2+b^2 = p > 1$. Thus p is not a prime complex integer.

The factors $a+bi$ and $a-bi$, however, are prime complex integers. In fact, if $a+bi = \mu\nu$, where

$$N(\mu) > 1 \quad \text{and} \quad N(\nu) > 1, \tag{19}$$

then $p = N(a+bi) = N(\mu)N(\nu)$, which is impossible, since p is a prime.

From this we conclude that *the complex factors of primes of the form* $4k+1$, *where* k *is a natural number, are prime complex numbers.*

It is easy to see that these factors are not associated with each other. In fact, the identity $a+bi = a-bi$ is impossible, since it implies $b = 0$ and $p = a^2$. The identity $a+bi = -(a-bi)$ is also impossible because it implies $a = 0$, $p = b^2$. If $a+bi = i(a-bi)$, then $a = b$ and so $p = 2a^2$, which is impossible. Finally, if $a+bi = -i(a-bi)$, then $a = -b$ and so $p = 2a^2$, which is impossible.

As for the *primes of the form* $4k+3$, *where* k *is a non-negative rational integer*, we show that they *are prime when regarded as complex integers.*

In fact, if a prime $p = 4k+3$ were a product of two complex integers with norms greater than 1, then

$$p = (a+bi)(c+di),$$

whence, passing to the norms,

$$p^2 = (a^2+b^2)(c^2+d^2),$$

where $a^2+b^2 > 1$ and $c^2+d^2 > 1$. Since p is a prime, this would give $p = a^2+b^2$, but this is impossible for any prime of the form $4k+3$.

Thus we see that among the primes precisely the primes of the form $4k+3$ are prime complex integers. Other prime complex integers are the number $1+i$ and the conjugate complex factors of the primes of the form $4k+1$.

In virtue of what we proved above, any natural number > 1 is a product of prime complex integers of one of the sorts we have just listed or of their associates.

It is clear that there cannot be any other prime complex integers because, if π were such a prime, then, in virtue of the uniqueness of the decomposition of a complex integer into prime complex integers, π would not be a complex prime divisor of any natural number. But $\pi\pi' = N(\pi)$, which is a contradiction.

We have thus proved

THEOREM 7. *The complex prime integers are those of the following three classes and their associates:*

1. $1+i$,
2. *the complex prime factors of the primes of the form* $4k+1$,
3. *primes of the form* $4k+3$.

Here are the prime complex integers (one out of each of the four associates) whose norms are less than 100:

$$1+i,\quad 1\pm 2i,\quad 3,\quad 2\pm 3i,\quad 1\pm 4i,\quad 2\pm 5i,\quad 1\pm 6i,$$
$$4\pm 5i,\quad 7,\quad 2\pm 7i,\quad 5\pm 6i,\quad 3\pm 8i,\quad 5\pm 8i,\quad 4\pm 9i.$$

Two complex primes whose difference is 2 are said to form a pair of *twin* complex primes. For example, $4+i$, $6+i$; $3i$, $2+3i$; $3+2i$, $5+2i$; $7i$, $2+7i$. There are known twin complex primes that form arithmetical progressions of difference 2 consisting of three terms. For example, $2+i$, $4+i$, $6+i$ or $1+2i$, $3+2i$, $5+2i$.

Conjecture H (Chapter III, § 8) implies that there exist infinitely many pairs of complex twin primes. In fact, let $f_1(x) = x^2-2x+2$, $f_2(x) = x^2+2x+2$. The polynomials $f_1(x)$ and $f_2(x)$ have no rational roots and consequently they are irreducible. We also have $f_1(0)f_2(0) = 4$, $f_1(1)f_2(1) = 5$, which shows that the condition C is satisfied. Therefore, in view of Conjecture H, there exist infinitely many natural numbers x such that $f_1(x)$ and $f_2(x)$ are both prime. But $f_1(x) = (x-1)^2+1$, $f_2(x) = (x+1)^2+1$ and x must be odd since otherwise $2|f_2(x)$ and $f_2(x) > 2$, whence $f_2(x)$ would be composite. Consequently, the numbers $f_1(x)$ and $f_2(x)$ are both of the form $4k+1$ and so the numbers $x-1\pm i$ and $x+1\pm i$ are prime complex integers, their difference being equal to 2. Thus we have obtained an infinite sequence of different pairs of complex twin primes. Such pairs are obtained, for example, for $x = 3, 5, 15, 25, 55, \ldots$ However, there are pairs of complex twin primes that are not obtained in this way, for example, $1+2i$, $3+2i$ or $3+8i$ and $5+8i$.

Pairs of complex twin primes have been considered by D. Shanks [1].

5. The factorization of complex integers into complex prime factors

We now show a method how a complex integer z can be represented as the product of complex primes.

Let $N(z) = n$. Any prime factor of the number z is of course a prime factor of its norm $n = zz'$. Complex prime factors of the natural number n can easily be obtained by finding its rational prime factors. In fact, let

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}, \tag{20}$$

where the p's are primes of the form $4t+1$ (1) and the q's are primes of the form $4t+3$. Let π_j and π'_j, $j = 1, 2, \dots, k$, denote the conjugate complex prime factors of the number p_j. Let $\pi_j = a+bi$ and $\pi'_j = a-bi$; then $p_j = a^2+b^2$. Then the factorization of n into complex prime factors is as follows:

$$n = (-i)^{\alpha}(1+i)^{2\alpha} \pi_1^{\alpha_1} \pi_1'^{\alpha_1} \pi_2^{\alpha_2} \pi_2'^{\alpha_2} \dots \pi_k^{\alpha_k} \pi_k'^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}. \tag{21}$$

Since $n = zz'$, we see that

$$z = i^{\nu}(1+i)^{\lambda} \pi_1^{\lambda_1} \pi_1'^{\lambda'_1} \pi_2^{\lambda_2} \pi_2'^{\lambda'_2} \dots \pi_k^{\lambda_k} \pi_k'^{\lambda'_k} q_1^{\mu_1} q_2^{\mu_2} \dots q_l^{\mu_l}, \tag{22}$$

where ν is one of the numbers 1, 2, 3, 4, the remaining exponents λ, λ_1, $\lambda'_1, \dots, \lambda_k, \lambda'_k, \mu_1, \dots, \mu_l$ being non-negative integers. Passing to the norms in (22), in virtue of the equalities $N(\pi_j) = p_j$ and $N(q_j) = q_j^2$, we obtain

$$N(z) = 2^{\lambda} p_1^{\lambda_1+\lambda'_1} p_2^{\lambda_2+\lambda'_2} \dots p_k^{\lambda_k+\lambda'_k} q_1^{2\mu_1} q_2^{2\mu_2} \dots q_l^{2\mu_l},$$

whence, by (21) and the fact that $N(z) = n$, comparing the exponents on equal primes, we obtain

$$\begin{gathered} \lambda = \alpha, \quad \lambda_1+\lambda'_1 = \alpha_1, \quad \lambda_2+\lambda'_2 = \alpha_2, \quad \dots, \quad \lambda_k+\lambda'_k = \alpha_k, \\ 2\mu_1 = \beta_1, \quad 2\mu_2 = \beta_2, \quad \dots, \quad 2\mu_l = \beta_l. \end{gathered} \tag{23}$$

Equalities (23) show that all the exponents β must be even.

Thus we reach the conclusion that, *if a natural number n is the norm of a complex integer, then in the factorization of n into primes the primes of the form $4k+3$ have even exponents.*

Further, equalities (23) give

$$\lambda = \alpha, \quad \mu_1 = \tfrac{1}{2}\beta_1, \quad \mu_2 = \tfrac{1}{2}\beta_2, \quad \dots, \quad \mu_l = \tfrac{1}{2}\beta_l.$$

Thus the exponents λ, μ_1, μ_2, ..., μ_l are uniquely defined.

In order to establish the exponents λ_j and λ'_j, where $j = 1, 2, \dots, k$, we use another rule which can be deduced as follows.

---

(1) Here p_n does not denote the nth prime.

Let k_j be the greatest exponent for which $p_j^{k_j} \mid z$, i.e. let k_j be the greatest exponent for which $p_j^{k_j}$ divides both a and b, where $z = a+bi$. Then

$$(24)\qquad \left.\begin{aligned} \lambda_j &= \alpha_j - k_j \\ \lambda_j' &= k_j \end{aligned}\right\} \text{if } p_j^{k_j}\pi_j \mid z, \qquad \left.\begin{aligned} \lambda_j' &= \alpha_j - k_j \\ \lambda_j &= k_j \end{aligned}\right\} \text{if } p_j^{k_j}\pi_j \nmid z.$$

In fact, it follows from the definition of the exponent k_j that the complex integer $z/p_j^{k_j}$ cannot be divisible by π_j and π_j' simultaneously, because, if it could, then, since $(\pi_j, \pi_j') = 1$, it would be divisible by $\pi_j \pi_j' = p_j$, whence $p_j^{k_j+1} \mid z$, contrary to the definition of k_j.

Consequently if $\pi_j \mid (z/p_j^{k_j})$, then the number $z/p_j^{k_j}$ is not divisible by π_j'. Hence, in view of $p_j^{k_j} = \pi_j^{k_j}\pi_j'^{k_j}$, it follows by (22) that $\lambda_j' = k_j$, whence, by (23), $\lambda_j = \alpha_j - k_j$. If the number $z/p_j^{k_j}$ is not divisible by π_j, then, as one easily sees, $\lambda_j = k_j$ and $\lambda_j' = \alpha_j - k_j$.

This completes the proof of the rule provided by (24).

Finally, the exponent ν is easily found by a simple division of z by the product of the prime factors whose exponents have already been defined.

EXAMPLES. 1. Let $z = 22+7i$. We then have

$$N(z) = 484+49 = 533 = 13\cdot 41, \quad p_1 = 13 = 2^2+3^2,$$
$$p_2 = 41 = 4^2+5^2.$$

Consequently,

$$z = i^\nu \pi_1^{\lambda_1} \pi_1'^{\lambda_1'} \pi_2^{\lambda_2} \pi_2'^{\lambda_2'},$$

where $\pi_1 = 2+3i, \pi_1' = 2-3i, \pi_2 = 4+5i, \pi_2' = 4-5i$. Clearly, $k_1 = k_2 = 0$. The number

$$z/\pi_1 = (22+7i)/(2+3i) = (22+7i)(2-3i)/13 = 5-4i$$

is a complex integer, and so $\lambda_1 = \alpha_1 - 0 = 1, \lambda_1 = 0$. Similarly, the quotient z/π_2 could be calculated, but it is sufficient to note the number $5-4i$ is a prime complex integer. Hence immediately,

$$22+7i = (2+3i)(5-4i)$$

is the required factorization.

2. Let $z = 19+17i$. We then have

$$N(z) = 361+289 = 650 = 2\cdot 5^2\cdot 13 = 2\cdot p_1^2\cdot p_2.$$

Consequently,

$$z = i^\nu(1+i)\pi_1^{\lambda_1} \pi_1'^{\lambda_1'} \pi_2^{\lambda_2} \pi_2'^{\lambda_2'},$$

where $\pi_1 = 1+2i, \pi_1' = 1-2i, \pi_2 = 2+3i, \pi_2' = 2-3i, \alpha_1 = 2, \alpha_2 = 1$.

Since neither $5 \mid z$, nor $13 \mid z$, we have $k_1 = k_2 = 0$. Moreover the number $(19+17i)/(1+2i)$ is not a complex integer, and so $\lambda_1 = 0$ and $\lambda_1' = 2$. The number $(19+17i)/(2+3i)$ is not a complex integer either. Therefore $\lambda_2 = 0$ and $\lambda_2' = 1$. We then have

$$z = i^\nu(1+i)(1-2i)^2(2-3i),$$

where a simple division shows that $v = 2$. Therefore the required factorization is

$$19+17i = (1+i)(1-2i)^2(-2+3i).$$

3. Let $z = 10+100i$. We may write $z = 10(1+10i)$ and since

$$10 = 2\cdot 5 = -i(1+i)^2(1+2i)(1-2i),$$

it is sufficient to find the factorization of $1+10i$. We have $N(1+10i) = 101$. This is a prime of the form $4k+1$. Hence, by Theorem 7, $1+10i$ is a prime complex integer. Therefore

$$10+100i = -i(1+i)^2(1+2i)(1-2i)(1+10i).$$

EXERCISE. Find the factorization into prime complex integers of the complex integers: $1+7i$, $9+i$, $7+9i$, $107+198i$, $10+i$, $7+24i$.

ANSWER. $1+7i = -i(1+i)(1+2i)^2$, $9+i = -i(1+i)(4+5i)$, $7+9i = (1+i)(1+2i)(3-2i)$, $107+198i = -(1+6i)^3$, $10+i = 10+i$, $7+24i = -(1+2i)^4$.

6. The number of complex integers with a given norm

Now we are going to investigate the question how many there are complex integers with norms equal to a given natural number n.

The question is important not only in itself; another source of its applicability lies in the fact that it is equivalent to the problem of finding the number of the pairs of rational integers x, y for which $x^2+y^2 = n$. In other words, the number $\tau(n)$ of complex integers with norms equal to n is equal to the number of representations of the number n as the sum of the squares of two rational integers. Therefore the function $\tau(n)$ appears to be the same as has already been investigated in Chapter XI, § 2.

Let (20) be the factorization of the number n into primes and let (21) be its factorization into prime complex integers. As we have already shown (cf. § 5), $N(z) = n$ holds only in the case where the exponents β_j, $j = 1, 2, \ldots, l$ are even. Suppose that this condition is satisfied. Then, as we have learned, a number z with the norm n has a factorization into complex primes as in (22), equalities (23) for the exponents being satisfied, and v is one of the numbers 1, 2, 3, 4. Conversely, if λ, λ_1, λ_1', λ_2, $\lambda_2' \ldots, \lambda_k, \lambda_k'$, $\mu_1, \mu_2, \ldots, \mu_l$ is an arbitrary system of non-negative integers which satisfy equalities (23) and v is one of the numbers 1, 2, 3, 4, then the number z, uniquely defined by (22), has the norm n. Thus, since the numbers λ, $\mu_1, \mu_2, \ldots, \mu_l$ are uniquely defined by conditions (23) the question about the number of different complex integers whose norms are equal to n is equivalent to the question about the number of different systems of non-negative $\nu, \lambda_1, \lambda_1', \lambda_2, \lambda_2', \ldots, \lambda_k, \lambda_k'$ that satisfy the conditions

$$1 \leqslant \nu \leqslant 4, \quad \lambda_1 + \lambda_1' = \alpha_1, \quad \lambda_2 + \lambda_2' = \alpha_2, \quad \ldots, \quad \lambda_k + \lambda_k' = \alpha_k.$$

There are four possible values for the number ν: 1, 2, 3, 4. For λ_1, λ_1' we have the following $\alpha_1 + 1$ possibilities: $0, \alpha_1$; $1, \alpha_1 - 1$; $2, \alpha_1 - 2$; ...; $\alpha_1, 0$. Similarly, there are $\alpha_2 + 1$ possible values for λ_2, λ_2' and so on. This shows that

$$\tau(n) = 4(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1). \tag{25}$$

This formula has been obtained under the assumption that the exponents on the primes of the form $4t + 3$ in the factorization of n into primes are all even. Otherwise, the equation $N(z) = n$ is not solvable in complex integers z, and so $\tau(n) = 0$. Thus we have proved the following

THEOREM 8. *If a natural number n is factorized into prime factors as in* (20), *then the number* $\tau(n)$ *of the representations of n as the sum of the squares of two rational integers is equal to* $4(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$ *provided the exponents on the primes of the form* $4t + 3$ *that appear in the factorization are even. Otherwise* $\tau(n) = 0$.

The theorem obtained in Chapter XI, § 1, in a different way is an immediate consequence of Theorem 8.

In particular, if n is a prime of the form $4t + 1$, then $\tau(n) = 8$, whence, immediately, Theorem 9 of Chapter V follows.

Now let $f(h)$ be a function defined as follows:

$$f(h) = \begin{cases} 0 & \text{if } h \text{ is even,} \\ +1 & \text{if } h \text{ is of the form } 4t+1, \\ -1 & \text{if } h \text{ is of the form } 4t+3. \end{cases} \tag{26}$$

It is easy to see that for any rational integers a, b

$$f(ab) = f(a)f(b).$$

Hence, if

$$n = h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_k^{\alpha_k}$$

is the factorization of n into prime factors, then, as is easy to see,

$$\sum_{d \mid n} f(d) = (f(1) + f(h_1) + f(h_1^2) + \ldots + f(h_1^{\alpha_1})) \ldots (f(1) + f(h_k) + \ldots + f(h_k^{\alpha_k})).$$

According to (26) we have

$$f(1) + f(2) + f(2^2) + \ldots + f(2^\alpha) = 1.$$

If $h = 4t+1$, then

$$f(1)+f(h)+f(h^2)+ \dots +f(h^\alpha) = \alpha+1.$$

If $h = 4t+3$, then

$$\begin{aligned} f(1)+f(h)+f(h^2)+ \dots +f(h^\alpha) &= 1-1+1- \dots +(-1)^\alpha \\ &= \frac{1+(-1)^\alpha}{2}. \end{aligned} \tag{27}$$

In virtue of the formula for $\sum\limits_{d|n} f(d)$ we have

$$\sum_{d|n} f(d) = \prod_{h_i \equiv 1 \pmod 4} (\alpha_i + 1)$$

whence, by Theorem 8,

$$\tau(n) = 4\sum_{d|n} f(d), \tag{28}$$

provided all prime factors of n of the form $4t+3$ have even exponents in the factorization of n into primes. Otherwise, by (27),

$$\sum_{d|n} f(d) = 0,$$

which, by Theorem 8, shows that equality (28) is valid. Consequently it is valid for any n. This can be formulated in the following *theorem of Jacobi.*

THEOREM 9. *The number of representations of a natural number n as the sum of the squares of two rational integers is equal to the difference between the number of the divisors of the form* $4t+1$ *of n and the number of divisors of the form* $4t+3$ *of n, multiplied by four.*

In fact, in (28) the summand $+1$ appears as many times as there are divisors of the form $4t+1$ of number n; the summand -1 appears as many times as there are divisors of the form $4t+3$ of number n.

By (28) we obtain

$$\frac{1}{4}\sum_{n=1}^{[x]} \tau(n) = \sum_{k=1}^{[x]} f(k)\left[\frac{x}{k}\right]. \tag{29}$$

Since the summands $f(d)$ appear in the sum $\sum\limits_{n=1}^{[x]} \sum\limits_{d|n} f(d)$ as many times as there are numbers $n \leqslant s$ which $d|n$, i.e. $\left[\frac{x}{d}\right]$ times.

In virtue of formula (6) of Chapter XI, § 2, we have

$$\frac{1}{4}\sum_{n=1}^{[x]}\tau(n)=\sum_{k=0}^{[\sqrt{x}]}[\sqrt{x-k^2}],$$

whence

$$\sum_{k=0}^{[\sqrt{x}]}[\sqrt{x-k^2}]=\sum_{k=1}^{[\sqrt{x}]}f(k)\left[\frac{x}{k}\right], \tag{30}$$

and so

$$[\sqrt{x}]+[\sqrt{x-1^2}]+[\sqrt{x-2^2}]+\ldots$$
$$=\left[\frac{x}{1}\right]-\left[\frac{x}{3}\right]+\left[\frac{x}{5}\right]-\left[\frac{x}{7}\right]+\ldots,$$

where the sequence of summands on the left-hand side breaks up at the last positive term under the sign of square root, and that on the right-hand side breaks up at the last fraction for which the numerator is not less than the denominator.

This is known under the name of *Liouville's identity.*

In particular, for $x = 10$, we have

$$[\sqrt{10}]+[\sqrt{9}]+[\sqrt{6}]+[\sqrt{1}]=[\tfrac{10}{1}]-[\tfrac{10}{3}]+[\tfrac{10}{5}]-[\tfrac{10}{7}]+[\tfrac{10}{9}],$$

whence, indeed, $3+3+2+1 = 10-3+2-1+1$.

Liouville's identity implies Jacobi's theorem the other way round.

It is worth-while to mention that, by inequalites of Chapter XI, § 2, Liouville's identity implies Leibniz's expansion of the number π:

$$\frac{\pi}{4}=\frac{1}{1}-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\ldots$$

in an elementary way.

What is astonishing in this expansion is the rôle of the consecutive odd numbers that appear in the denominators of the summands of the expansion. The ancients used to say "Numero impari deus gaudet". In a purely arithmetical way we have obtained a formula for the most important geometric constant: the ratio of the circumference of a circle to its diameter; the formula which is simply a series of reciprocals of the consecutive odd natural numbers equipped with alternating signs.

Another formula for π built up of the consecutive odd numbers is that due to Euler,

$$\frac{\pi^2}{8}=\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\frac{1}{9^2}+\ldots$$

This formula can also be obtained in an elementary way. Of the other formulae for the number π that are proved in analysis we mention here the following:

Wallis's formula

$$\frac{\pi}{4} = \left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{7^2}\right)\left(1-\frac{1}{9^2}\right)\ldots,$$

Euler's formula

$$\frac{\pi^3}{32} = \frac{1}{1^3}-\frac{1}{3^3}+\frac{1}{5^3}-\frac{1}{7^3}+\frac{1}{9^3}-\ldots,$$

and the *formula of Brouncker*

$$\frac{4}{\pi} = 1+\frac{1^2\mid}{\mid 2}+\frac{3^2\mid}{\mid 2}+\frac{5^2\mid}{\mid 2}+\frac{7^2\mid}{\mid 2}+\frac{9^2\mid}{\mid 2}+\ldots$$

7. Jacobi's four-square theorem

Now we are going to prove a theorem of Jacobi that concerns the representations of a number as the sum of four squares.

At first we consider the case where the natural number n is of the form $n = 4u$. Let

$$4u = x^2+y^2+z^2+t^2 \tag{31}$$

be a representation of $4u$ as the sum of four odd squares.

It is clear, that, since x, y, z, t are odd,

$$x^2+y^2 = 2u' \quad \text{and} \quad z^2+t^2 = 2u'', \tag{32}$$

where u' and u'' are odd natural numbers. In view of (31) and (32) we have

$$2u = u'+u''. \tag{33}$$

On the other hand, if w is an odd number and $2w = a^2+b^2$, then the numbers a, b are odd. The reason is that if a, b were both even, then $2w$ would be divisible by 4, contrary to the assumption that w is odd. If one of the numbers a, b were odd, the other being even, then the number $2w$ would be odd, which is clearly false.

Thus we see that, in order to find all the representations of the number $4u$ as the sum of four odd squares, it is sufficient to find all possible representations of $2u$ as sums of two odd numbers u' and u'', and then to find the representations of either of the numbers u', u'' as the sum of two squares.

Denote by $\theta(4u)$ the number of all possible representations of the number $4u$ as the sum of four odd squares.

For any pair of two fixed odd numbers u' and u'' that satisfy equality (33), by (28) and the equality $\tau(2m) = \tau(m)$, $m = 1, 2, \ldots$, which follows from (25), the number of all coresponding representations of the number $4u$ as the sum of four squares of odd numbers is

$$\tau(2u')\,\tau(2u'') = 16 \sum_{d'|u'} f(d') \sum_{d''|u''} f(d'').$$

Hence, the total number of such representations is

$$(34) \qquad \theta(4u) = 16 \sum_{u'+u''=2u} \Big(\sum_{d'|u'} f(d') \cdot \sum_{d''|u''} f(d'')\Big),$$

where the summation in the first sum extends all over the pairs u', u'', of natural numbers that satisfy (33). Since any divisor of any odd number is odd, by (26), we have

$$\sum_{d'|u'} f(d') = \sum_{d'|u'} (-1)^{\frac{1}{2}(d'-1)}$$

and similarly

$$\sum_{d''|u''} f(d'') = \sum_{d''|u''} (-1)^{\frac{1}{2}(d''-1)}$$

This applied to (34) gives

$$(35) \qquad \theta(4u) = 16 \sum_{u'+u''=2u} \Big(\sum_{d'|u'} (-1)^{\frac{1}{2}(d'-1)} \cdot \sum_{d''|u''} (-1)^{\frac{1}{2}(d''-1)}\Big).$$

The product of the sums in brackets can be expressed as the sum of products according to the rule

$$\sum_{m=1}^{p} a_m \sum_{n=1}^{q} b_n = (a_1 + a_2 + \ldots + a_p)(b_1 + b_2 + \ldots + b_q) = \sum_{m=1}^{p} \sum_{n=1}^{q} a_m b_n.$$

Thus (35) gives

$$(36) \qquad \theta(4u) = 16 \sum_{u'+u''=2u} \sum_{d'|u'} . \sum_{d''|u''} (-1)^{\frac{1}{2}(d'-1)+\frac{1}{2}(d''-1)}.$$

In virtue of the identity

$$\tfrac{1}{2}(d'-1) + \tfrac{1}{2}(d''-1) = \tfrac{1}{2}(d'-d'') + d'' - 1$$

and since d'' as a divisor of an odd number is odd, we have

$$(-1)^{\frac{1}{2}(d'-1)+\frac{1}{2}(d''-1)} = (-1)^{\frac{1}{2}(d'-d'')}$$

Thus (36) turns into

$$(37) \qquad \theta(4u) = 16 \sum_{u'+u''=2u} \sum_{d'|u'} \sum_{d''|u''} (-1)^{\frac{1}{2}(d'-d'')}.$$

For any pair of odd natural numbers u' and u'' that satisfy (33) and for any pair of divisors d' and d'', we denote the corresponding complementary divisors by δ', δ''. We then have

$$u' = d'\delta', \qquad u'' = d''\delta''. \tag{38}$$

Accordingly, by (33), we have

$$2u = d'\delta' + d''\delta'', \tag{39}$$

where δ' and δ'' as divisors of odd numbers are odd. Consequently, to each summand of the sum (37) corresponds the unique system of four odd natural numbers

$$d', \quad d'', \quad \delta', \quad \delta'', \tag{40}$$

which satisfy equality (39). It is clear that, conversely, since the first two of the indices d', d'', δ', δ'' that define the summand are given and the other two are defined by (38), the unique summand of the sum (37) corresponds to any system of natural numbers (40) which satisfy (39).

Therefore we may write

$$\theta(4u) = 16 \sum_{d'\delta' + d''\delta'' = 2u} (-1)^{\frac{1}{2}(d'-d'')} \tag{41}$$

where the summation on the right-hand side extends all over the systems (40) consisting of four odd numbers that satisfy (39).

Now we divide the summands of (41) into two classes, the first consisting of the summands for which $d' = d''$ and the second of those for which $d' \neq d''$.

Given an odd natural number d, we are going to calculate the sum of the summands of (41) for which $d' = d'' = d$. As follows from (39), d is a divisor of the number $2u$ and, being odd, it must be a divisor of u. We then have $u = d\delta$, whence by (39)

$$2\delta = \delta' + \delta''.$$

This shows that the number of the summands of (41) for which $d' = d'' = d$ is equal to the number of representations of 2δ as the sum of two odd natural numbers, this being equal to δ. But since any such summand is equal to $+1$, the sum of the summands is equal to $\delta = u/d$.

From this we infer that the sum of the summands that belong to the first class is

$$\sum_{d|u} \frac{u}{d} = \sum_{d|u} d = \sigma(u).$$

The summands that belong to the second class are again divided into two groups, the first consisting of the summands for which $d' > d''$, the second of those for which $d'' > d'$. To each summand defined by a system of the first group corresponds the unique summand of the second group defined by the system d', d'', δ', δ'' and *vice versa*. Therefore it is sufficient to calculate the sum of the summands that belong to the first group and multiply it by 2.

Let

$$\vartheta = \left[\frac{d''}{d'-d''}\right]. \tag{42}$$

To any summand of the first group defined by system (40) corresponds a summand defined by the system

$$d_1, \quad d_2, \quad \delta_1, \quad \delta_2, \tag{43}$$

where

$$\begin{aligned} d_1 &= \delta' + (\vartheta+1)(\delta'+\delta''), & d_2 &= \delta' + \vartheta(\delta'+\delta''), \\ \delta_1 &= d'' - \vartheta(d'-d''), & \delta_2 &= (\vartheta+1)(d'-d'') - d''. \end{aligned} \tag{44}$$

First of all we show that system (43) defined by formulae (44) indeed defines a summand of the first group. Since ϑ is an integer and the numbers of (40) are odd, the numbers $\delta'+\delta''$ and $d'-d''$ are even. Hence, by (44), we see that the numbers of (43) are odd integers.

By (42), the number ϑ is non-negative since, for the summands of the first group, $d' > d''$. Consequently, by (44), the numbers d_1 and d_2 are positive. Moreover, by (42),

$$\frac{d''}{d'-d''} - 1 < \vartheta \leqslant \frac{d''}{d'-d''},$$

which, multiplied by $d'-d'' > 0$, gives

$$d'' - (d'-d'') < \vartheta(d'-d'') \leqslant d''.$$

This, by (44), shows that $\delta_1 \geqslant 0$ and $\delta_2 > 0$. But the number δ_1, being odd, cannot be equal to zero, consequently $\delta_1 > 0$.

Thus we see that the four numbers of (43) are odd and positive.

Further, by (44), we find

$$d_1 - d_2 = \delta' + \delta''. \tag{45}$$

This shows that $d_1 > d_2$. Moreover,

$$\delta_1 + \delta_2 = d' - d'', \tag{46}$$

whence, by (45) and the identity

$$d_1\delta_1+d_2\delta_2 = d_1(\delta_1+\delta_2)-(d_1-d_2)\delta_2,$$

we obtain

$$d_1\delta_1+d_2\delta_2 = d_1(d'-d'')-(\delta'+\delta'')\delta_2.$$

Hence, in virtue of (44), we have

$$d_1\delta_1+d_2\delta_2 = \delta'(d'-d'')+(\delta'+\delta'')d'',$$

which, by (39), gives

$$d_1\delta_1+d_2\delta_2 = 2u.$$

From this we conclude that system (43) indeed defines a summand of the first group.

System (43) is different from system (40). This is because of the fact that, if the two systems were identical, then by (45) we would have $d'-d'' = \delta'+\delta''$, whence, by (39)

$$2u = (d'-d'')\delta'+(\delta'+\delta'')d'' = (\delta'+\delta'')(\delta'+d'')$$

and so, since the numbers $\delta'+\delta''$ and $\delta'+d''$ are even, $2u$ would be divisible by 4, contrary to the assumption that u is odd.

To find the numbers (40) we solve the equations (44), whence, by (45) and (46) we obtain

$$\delta' = d_1-(\vartheta+1)(d_1-d_2) = d_2-\vartheta(d_1-d_2), \quad d'' = \delta_1+\vartheta(\delta_1+\delta_2).$$

Hence, by (45) and (46),

$$\delta'' = d_1-d_2-\delta' = (\vartheta+1)(d_1-d_2)-d_2,$$
$$d' = \delta_1+\delta_2+d'' = \delta_1+(\vartheta+1)(\delta_1+\delta_2).$$

In virtue of formulae (44) and (42) we obtain

$$(47)\qquad \vartheta_1 = \left[\frac{d_2}{d_1-d_2}\right] = \left[\frac{\delta'+\vartheta(\delta'+\delta'')}{\delta'+\delta''}\right] = \left[\frac{\delta'}{\delta'+\delta''}+\vartheta\right] = \vartheta$$

because ϑ is an integer and $\delta'/(\delta'+\delta'')$ is a proper fraction. Thus, finally, we obtain

$$(48)\qquad \begin{aligned} d' &= \delta_1+(\vartheta_1+1)(\delta_1+\delta_2), & d'' &= \delta_1+\vartheta_1(\delta_1+\delta_2),\\ \delta' &= d_2-\vartheta_1(d_1-d_2), & \delta'' &= (\vartheta_1+1)(d_1-d_2)-d_2. \end{aligned}$$

Comparing formulae (47) and (48) with formulae (42) and (44) we come to the conclusion that systems (43) and (40) correspond to each other with respect to the correspondence defined above. In other words, the correspondence we have defined orders the summands of the first group in pairs in such a way that each pair consists of two summands, one defined by system (40) and the other by (43), linked together by formulae (44).

Let us calculate the sum of the summands that belong to the same pair, i.e. the sum

$$(-1)^{(d'-d'')/2}+(-1)^{(d_1-d_2)/2}, \tag{49}$$

where d', d'', d_1 and d_2 are linked together by formulae (44).

In virtue of (39) and (45) we have $2u = (d'-d'')\,\delta' + (d_1-d_2)\,d''$, and so

$$\frac{d'-d''}{2}\,\delta' + \frac{d_1-d_2}{2}\,d'' \doteq u.$$

Hence, since the numbers δ', d'' and u are odd,

$$\frac{d'-d''}{2} + \frac{d_1-d_2}{2} \equiv 1 \pmod 2.$$

This proves that sum (49) is equal to zero. In other words, this means that the summands that belong to the same pair cancel each other.

Thus the sum of the summands of the first group, and consequently the total sum of the summands of the second class in the first partition into two classes is zero. As we have already proved, the sum of the summands of the first class is equal to $\sigma(u)$; therefore, by (41), we obtain

THEOREM 10. *If u is an odd natural number, then*

$$\theta(4u) = 16\sigma(u).$$

This theorem was first formulated (in a slightly different way) and proved by Jacobi [1]. The proof we have presented here, simpler than the original one of Jacobi, is due to Dirichlet [1] (cf. also Bachmann [2], pp. 349-354).

Now let

$$u = \xi^2+\eta^2+\zeta^2+\vartheta^2 \tag{50}$$

be a representation of an odd natural number u as the sum of four squares and let

$$\begin{aligned} x' &= \xi+\eta+\zeta+\vartheta, & y' &= \xi+\eta-\zeta-\vartheta,\\ z' &= \xi-\eta+\zeta-\vartheta, & t' &= \xi-\eta-\zeta+\vartheta. \end{aligned} \tag{51}$$

Since, clearly, $w^2 \equiv w \pmod 2$ for any integer w, by (50), $x' \equiv u \pmod 2$, which in view of the fact that u is odd proves that x' is odd. Further, since formulae (50) imply that

$$y' = x' - 2(\zeta + \vartheta), \qquad z' = x' - 2(\eta + \vartheta), \qquad t' = x' - 2(\eta + \zeta),$$

all the four numbers x', y', z', t' are odd. In virtue of (50) and (51) we can easily verify that

$$x'^2 + y'^2 + z'^2 + t'^2 = 4u.$$

Therefore the system

$$x',\ y',\ z',\ t' \tag{52}$$

defined by (50) gives a representation of the number $4u$ as the sum of four odd squares.

On the other hand, let

$$\begin{aligned} x'' &= -\xi + \eta + \zeta + \vartheta, & y'' &= \xi - \eta + \zeta + \vartheta, \\ z'' &= \xi + \eta - \zeta + \vartheta, & t'' &= \xi + \eta + \zeta - \vartheta. \end{aligned} \tag{53}$$

Here also the numbers

$$x'',\ y'',\ z'',\ t'' \tag{54}$$

are all odd and, again,

$$x''^2 + y''^2 + z''^2 + t''^2 = 4u.$$

It can be verified that systems (52) and (54) are different. This is because, by (51) and (53), we find

$$x' + y' + z' + t' = 4\xi, \qquad x'' + y'' + z'' + t'' = 2(\xi + \eta + \zeta + \vartheta) \tag{55}$$

and so, since $\xi + \eta + \zeta + \vartheta$ is odd, the sum of the numbers (52) is divisible by 4 while the sum of the numbers (54) is not.

In virtue of (51) and (53) to any representation of an odd number u as the sum of four squares correspond two different representations of the number $4u$ as the sum of four odd squares.

We now prove that to any representation (31) of the number $4u$ as the sum of four odd squares corresponds the unique representation of the number u as the sum of four squares.

In fact, the number

$$s = x + y + z + t,$$

being the sum of four odd numbers of (31), is even. We consider two cases:

(i) $s \equiv 0 \pmod 4$. Formulae (53) imply (55), consequently there are no integers $\xi, \eta, \zeta, \vartheta$ which satisfy (50) and are such that numbers x'', y'', z'', t'' defined by them are equal to x, y, z, t, respectively; this is because the existence of such integers would imply that s is not divisible by 4, contrary to the assumption. On the other hand, there exists precisely one system of integers $\xi, \eta, \zeta, \vartheta$ which satisfy (50) and for which

$$x = \xi+\eta+\zeta+\vartheta, \quad y = \xi+\eta-\zeta-\vartheta, \quad z = \xi-\eta+\zeta-\vartheta, \quad t = \xi-\eta+\zeta-\vartheta \tag{56}$$

because the validity of (56) implies the validity of

$$\frac{x+y+z+t}{4} = \xi, \quad \frac{x+y-z-t}{4} = \eta, \quad \frac{x-y+z-t}{4} = \zeta, \quad \frac{x-y-z+t}{4} = \vartheta, \tag{57}$$

and this proves that the system x, y, z, t corresponds to at most one system $\xi, \eta, \zeta, \vartheta$ for which formulae (57) hold. If we calculate the numbers $\xi, \eta, \zeta, \vartheta$ from formulae (57), we see that, in the case under consideration, the numbers obtained are integers which satisfy (56) and, by (31), they must satisfy (50), which proves that the system x, y, t, z corresponds to at least one such system.

Thus in case (i) there is a one-to-one correspondence between representations (31) and representations (50) of u as sums of four squares.

(ii) $s \equiv 2 \pmod 4$. In this case, since formulae (51) imply formulae (55), there are no integers $\xi, \eta, \zeta, \vartheta$ for which formulae (51) give a system

$$x' = x, \quad y' = y, \quad z' = z, \quad t' = t,$$

because otherwise the sum s would be divisible by 4, contrary to the assumption. On the other hand, there exists a unique system of integers $\xi, \eta, \zeta, \vartheta$ which satisfy (50) and are such that formulae

$$x = -\xi+\eta+\zeta+\vartheta, \quad . y = \xi-\eta+\zeta+\vartheta, \quad z = \xi+\eta-\zeta+\vartheta, \quad t = \xi+\eta+\zeta-\vartheta \tag{58}$$

are valid because the validity of.(58) implies the validity of

$$\frac{-x+y+z+t}{4} = \xi, \quad \frac{x-y+z+t}{4} = \eta, \quad \frac{x+y-z+t}{4} = \zeta, \quad \frac{x+y+z-t}{4} = \vartheta. \tag{59}$$

This proves that the system x, y, z, t corresponds to at most one system $\xi, \eta, \zeta, \vartheta$ for which formulae (59) hold. If the numbers $\xi, \eta, \zeta, \vartheta$ are calculated from formulae (59), we see that, in the case under consideration, they must be integers which satisfy (58). By (31), (58) implies that to the system x, y, z, t corresponds at least one such system $\xi, \eta, \zeta, \vartheta$.

Therefore, in case (ii), there is a one-to-one correspondence between representations (31) and representations (50) of the number u as sums of four squares.

In virtue of what we have proved above, the number of the representations of $4u$ as the sum of four odd squares is twice as large as the number $\tau_4(u)$ of representations of (odd) number u as the sum of four squares.

Hence, by Theorem 10, we obtain the validity of the formula

$$\tau_4(u) = 8\sigma(u) \tag{60}$$

for any odd natural number u. Thus we have

THEOREM 11. *The number of representations of an odd number as the sum of four squares is equal to the sum of its divisors multiplied by* 8.

Since the number of divisors of an odd number > 1 is at least 4, by Theorem 11 we see that any odd natural number > 1 has at least 32 representations as the sum of four squares. Since any odd square has precisely 8 representations as the sum of four squares three of which are equal to zero, we conclude that any odd square greater than 1 is a sum of four squares, at least two of them different from zero. Hence, by Lagrange's theorem, the following corollary is obtained.

COROLLARY. *Any natural number greater than* 1 *is a sum of four squares at least two of which are different from zero.*

Now, we are going to calculate the number of representations of the number $4u$ (where u is odd) as the sum of four squares.

Let

$$4u = x^2 + y^2 + z^2 + t^2 \tag{61}$$

be such a representation.

If one of the numbers x, y, z, t were even, the remaining ones being odd, or if one were odd, the remaining ones being even, then the sum of the squares of those numbers would be odd, contrary to (61).

If two of the numbers x, y, z, t were even, the other two being odd, then the sum of their squares would be of the form $4k+2$, contrary to formula (61).

Consequently, the numbers x, y, z, t must be all odd or all even.

The case where x, y, z, t are odd is fully described by theorem 10, which gives the number of representations of $4u$ as the sum of four odd squares. Thus it remains to calculate the number of representations of the number $4u$ as the sum of four even squares.

It is easy to see that to any such representation

$$4u = (2\xi)^2+(2\eta)^2+(2\zeta)^2+(2\vartheta)^2$$

corresponds a representation of u as the sum of four squares, namely

$$u = \xi^2+\eta^2+\zeta^2+\vartheta^2,$$

and *vice versa*. From this we infer that the number of representations of $4u$ as the sum of four even squares is equal to the number of representations of the number u as the sum of four squares, this, by (60) being equal to $8\sigma(u)$. Consequently, the total number of representations of the number $4u$ (where u is odd) as the sum of squares is

$$16\sigma(u)+8\sigma(u) = 24\sigma(u).$$

Hence

$$\tau_4(4u) = 24\sigma(u) \tag{62}$$

for any odd u.

Finally we calculate the number of representations of the number $2u$ as the sum of four squares. We shall prove that

$$\tau_4(2u) = \tau_4(4u). \tag{63}$$

In fact, if (61) is a representation of the number $4u$ (where u is odd) as the sum of four squares, then, as we have already learned, the numbers x, y, z, t are either all even or all odd. In any case

$$\xi = \frac{x+y}{2}, \quad \eta = \frac{x-y}{2}, \quad \zeta = \frac{z+t}{2}, \quad \vartheta = \frac{z-t}{2} \tag{64}$$

are integers. We rewrite formula (61) in the form

$$2u = \left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{z+t}{2}\right)^2+\left(\frac{z-t}{2}\right)^2,$$

whence the representation

$$2u = \xi^2+\eta^2+\zeta^2+\vartheta^2 \tag{65}$$

is obtained.

Thus to any representation (61) of the number $4u$ as the sum of four squares corresponds a representation (65) of the number $2u$ as the sum of four squares. On the other hand, it is clear that to any representation (65) of the number $2u$ as the sum of four squares corresponds precisely one representation (61) of the number $4u$ as the sum of four squares. The proof easily follows from the fact that, under the assumption that a representation (65) corresponds to a representation (61) with respect to the correspondence defined above, formulae (64) hold. So we obtain

$$\xi+\eta = x, \quad \xi-\eta = y, \quad \zeta+\vartheta = z, \quad \zeta-\vartheta = t,$$

and this defines uniquely the representation (64). Thus a one-to-one correspondence between the representations of the number $4u$ as the sum of four squares and the representations of the number $2u$ as the sum of four squares is defined. Formula (63) is thus proved. Hence, by (62), we obtain

$$\tau_4(2u) = 24\sigma(u) \tag{66}$$

for any odd u.

Our present aim is to calculate the number of the representations of the number $2^h u$ ($h = 3, 4, \ldots$; u is odd) as the sum of four squares.

Let

$$2^h u = x^2+y^2+z^2+t^2 \tag{67}$$

be such a representation. The numbers x, y, z, t cannot all be odd because, if they were, the right-hand side of (67) would be congruent to 4 (mod 8), while (since $h \geqslant 3$) the left-hand side is divisible by 8. Similarly, if two of the numbers were even, the other two being odd, then the right-hand side of (67) would be congruent to 2 (mod 4), which is impossible. From this we easily infer that all the numbers x, y, z, t must be even.

Let

$$x = 2\xi, \quad y = 2\eta, \quad z = 2\zeta, \quad t = 2\vartheta,$$

where ξ, η, ζ, ϑ are integers. In virtue of (67) we have

$$2^{h-2}u = \xi^2+\eta^2+\zeta^2+\vartheta^2. \tag{68}$$

Thus we see that to any representation (67) of the number $2^h u$ as the sum of four squares corresponds a representation (68) of the number $2^{h-2}u$ as the sum of four squares. On the other hand, it is clear that to any representation (68) of $2^{h-2}u$ precisely one representation of the number $2^h u$ corresponds, namely the representation

$$2^h u = (2\xi)^2+(2\eta)^2+(2\zeta)^2+(2\vartheta)^2.$$

Hence

$$\tau_4(2^h u) = \tau_4(2^{h-2}u) \tag{69}$$

for any $h \geqslant 3$ and any odd natural number u.

Now, let s be any natural number and u an odd natural number. If $s = 1$ or $s = 2$, then by (66) or by (62) respectively we obtain

$$\tau_4(2^s u) = 24\sigma(u). \tag{70}$$

If $s > 2$, we consider two cases.

(i) $s = 2k$. Then, by (69), we may write

$$\tau_4(2^s u) = \tau_4(2^{2k}u) = \tau_4(2^{2k-2}u) = \tau_4(2^{2k-4}u) = \ldots = \tau_4(2^2 u)$$

which, for this case, proves (70).

(ii) $s = 2k+1$. By (69) we have

$$\tau_4(2^s u) = \tau_4(2^{2k+1}u) = \tau_4(2^{2k-1}u) = \ldots = \tau_4(2^3 u) = \tau_4(2u),$$

whence, by (66), formula (70) follows.

Thus we see that formula (70) is true for any natural number s and any odd natural number u.

Formulae (60) and (70) can be formulated in one theorem. Accordingly we suppose that n is an arbitrary natural number, and by $\sigma^*(n)$ we denote the sum of divisors of the natural number n which are not divisible by 4.

If $n = u$ is odd, then none of the divisors of n is divisible by 4, so

$$\sigma^*(n) = \sigma(n). \tag{71}$$

If n is even, we put $n = 2^s u$, where s is a natural number and u is an odd natural number. It is clear that any divisor of the number $2^s u$ which is not divisible by 4 is a divisor of the number $2u$ and, conversely, any divisor of the number $2u$ is a divisor of the number $2^s u$ which is not divisible by 4.

Consequently

$$\sigma^*(n) = \sigma^*(2^s u) = \sigma(2u),$$

whence, since $(2, u) = 1$ implies

$$\sigma(2u) = \sigma(2)\,\sigma(u) = 3\sigma(u),$$

we have

$$\sigma^*(n) = 3\sigma(u). \tag{72}$$

Formulae (71) and (72) combined with formulae (60) and (70) prove the validity of

$$\tau_4(n) = 8\sigma^*(n) \tag{73}$$

for any natural number n. Thus we have shown the following

THEOREM 12. *The number of representations of a natural number n as the sum of four squares is equal to the sum of divisors which are not divisible by* 4 *of n multiplied by* 8.

Since any natural number has at least one divisor which is not divisible by 4 (e.g. the number 1), then as an immediate consequence of Theorem 12 we obtain the theorem stating that any natural number is a sum of four squares. This theorem was proved in Chapter XI in a different way.

An extensive list of references concerning the number of representations of number as the sum of any number of squares is given by E. Grosswald [2].

EXAMPLES. In virtue of (70) we have

$$\tau_4(100) = 24\sigma(25) = 24\frac{5^3-1}{5-1} = 24.31 = 744.$$

So the number 100 has 744 representations as the sum of four squares.

Similarly

$$\tau_4(90) = 24\sigma(45) = 24\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1} = 24\cdot 13\cdot 6 = 1872.$$

This is the greatest number of representations as the sum of four squares for a number $\leqslant 100$.

In the same way we obtain

$$\tau_4(7) = 8\sigma(7) = 8\cdot 8 = 64, \qquad \tau_4(6) = 24\sigma(3) = 24\cdot 4 = 96,$$
$$\tau_4(96) = 24\sigma(3) = 24\cdot 4 = 96, \quad \tau_4(1024) = \tau_4(2^{10}) = 24\sigma(1) = 24.$$

In virtue of (73) we easily obtain

$$\sum_{n=1}^{[x]} \tau_4(n) = 8S(x) - 32S\left(\frac{x}{4}\right),$$

where

$$S(x) = \sum_{k=1}^{[x]} k\left[\frac{x}{k}\right] = \frac{1}{2}\sum_{k=1}^{[x]} \left[\frac{x}{k}\right]\left(\left[\frac{x}{k}\right]+1\right).$$

From this we can easily deduce the inequality

$$\left|\sum_{n=1}^{[x]} \tau_4(n) - \frac{\pi^2 x^2}{2}\right| < 100x\sqrt{x},$$

valid for any integer x and obtain the formula of Euler

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots$$

in a purely arithmetical way.

BIBLIOGRAPHY

ABBOTT, H.L. and HANSON, D., [1] A problem of Schur and its generalizations, *Acta Arith.* **20** (1972) 175–187.

AIGNER, A., [1] Folgen der Art ar^n+b, welche nur teilbare Zahlen liefern, *Math. Nachr.* **23** (1961) 259–264.

ALAOGLU, L. and ERDÖS, P., [1] On highly composite and similar numbers, *Trans. Amer. Math. Soc.* **56** (1944) 448–469.

[2] A conjecture in elementary number theory, *Bull. Amer. Math. Soc.* **50** (1944) 881–882.

ANKENY, N.C., [1] Sums of three squares, *Proc. Amer. Math. Soc.* **8** (1957) 316–319.

ANNING, N.H. and ERDÖS, P., [1] Integral distances, *Bull. Amer. Math. Soc.* **51** (1945) 598–600.

AVANESOV, E.T., [1] Solution of a problem on figurate numbers (in Russian), *Acta Arith.* **12** (1966) 409–420.

AVANESOV, E.T. and GUSEV, V.A., [1] On a problem of Steinhaus (in Russian), *Mat. Chasopis* **21** (1971) 29–32.

[2] On Steinhaus' problem (in Russian), Manuscript deposited in VINITI file, cf. *Referativnyj Zhurnal Mat.* (1984), No 7A102.

BACHMANN, P., [1] Niedere Zahlentheorie, *Encyklopädie der Mathematischen Wissenschaften mit Einschluss ihrer Anwendungen* IC 1, 555–581, (Leipzig 1898–1904).

[2] *Niedere Zahlentheorie* II, (Leipzig 1901, reprint New York 1968).

BAILLIE, R. [1] Table of $\varphi(n)=\varphi(n+1)$, deposited in the UMT file, cf. *Math. Comp.* **30** (1976) 289–190.

[2] Solutions of $\varphi(n)=\varphi(n+1)$ for Euler's function, deposited in the UMT file, cf. *Math. Comp.* **32** (1978) 1326.

BAILLIE, R., CORMACK, G.V. and WILLIAMS, H.C., [1] The problem of Sierpiński concerning $k\cdot 2^n+1$, *Math. Comp.* **37** (1981) 229–231, Corrigendum, *ibid.* **39** (1982) 308.

BAKER, A., [1] Contributions to the theory of Diophantine equations II. The Diophantine equation $y^2=x^3+k$, *Philos. Trans. Roy. Soc. London* A **263** (1968) 193–208.

BAKER, C.L. and GRUENBERGER, F.J., [1] *The First Six Million Prime Numbers*, Madison, Wisc. 1959 (Microcards).

BALASUBRAMANIAN, R., DRESS, F. and DESHONILLES, J.-M., [1] Probléme de Waring pour les bicarrés, *C.R. Acad. Sci. Paris* (to appear).

BALOG, A., [1] $p+a$ without large prime factors, *Tagungsbericht* **44** (1984), *Mathematisches Forschungsbericht*, Oberwolfach.

BANG, A.S., [1] Über Summen von fünften Potenzen, *Neuvième congrès des math. Scand. 1938*, 292–296 (Helsinki 1939).

BANG, T., [1] Large prime numbers (in Danish), *Nordisk Mat. Tidskr.* **2** (1954) 157–168.

BAUMERT, L.D., [1] Sum-free sets, *Jet Propulsion Laboratory Res. Summary* No 36–10, 1 (1961) 16–18.

Beck, W.E. and Najar, R.M. [1] A lower bound for odd triperfects, *Math. Comp.* **38** (1982) 249–251.

Beeger, N.G.W.H., [1] On even numbers m dividing 2^m-2, *Amer. Math. Monthly* **58** (1951) 553–555.

[2] Cullen numbers, *Math. Tables Aids Comp.* **8** (1954) 188.

Behrend, F.A. [1] On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946) 331–332.

Bell, E.T. [1] Reciprocal arrays and diophantine analysis, *Amer. J. Math.* **55** (1933) 50–66.

Bendz, T.R., [1] *Öfver diophantiska ekvationen* $x^n+y^n=z^n$ *[On the Diophantine Equation* $x^n+y^n=z^n$*]*, Diss., (Upsala 1901).

Best, M.R. and te Riele, H.J.J., [1] *On a Conjecture of Erdös Concerning Sums of Powers of Integers*, Report NW 23/76, Mathematisch Centrum, (Amsterdam 1976).

Beyer, W.A., Metropolis, N. and Neugerard, J.R., [1] Square roots of integers 2 to 15 in various bases 2 to 10 : 88062 binary digits or equivalent, deposited in the UMT file, cf. *Math. Comp.* **23** (1969) 679.

Bieberbach, L., [1] Über Stifelsche magische Quadrate I, *Arch. Math.* **5** (1954) 4–11.

Blanuša, D., [1] Une interprétation géométrique du crible d'Erathostène (Serbo-Croatian), *Glasnik Mat. Fiz. Astronom. Društvo Mat. Fiz. Hrvatske* (2) **4** (1949) 201–202.

Bochner, S., [1] Remark on the Euclidean algorithm, *J. London Math. Soc.* **9** (1934) 4.

Bohman, J., [1] The number of primes less than a given limit, *Nordisk Tidskr. Informationsbehandling* (BIT), **12** (1972) 576–577.

[2] Some computational results regarding the prime numbers below 2000000000, *Nordisk Tidskr. Informationsbehandling* (BIT), **13** (1973) 242–244.

Borel, E., [1] Les probabilités dénombrables et leurs applications arithmétiques, *Rend. Circ. Mat. Palermo* **27** (1909) 247–271.

[2] Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilité en chaîne, *C.R. Acad. Sci. Paris* **230** (1950) 591–593.

Borho, W., [1] Befreundete Zahlen: ein zewitausend Jahre altes Thema der elementaren Zahlentheorie, in: *Lebendige Zahlen.* 5–38 (Basel–Boston–Stuttgart 1981).

Borozdkin, K.G., [1] On the problem of I.M. Vinogradov's constant (in Russian), *Trudy tretego vsesojuznogo matematicheskogo s'ezda*, Vol. I, 3, (Moskva 1956).

Bouniakowsky, V., [1] Notes sur quelques points de l'analyse indéterminée, *Bull. Acad. Sci. St. Pétersbourg* **6** (1848) 196–199.

[2] Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Acad. Sci. St. Pétersbourg Mém.* (6), *Sci. math. et phys.* **6** (1857) 305–329.

Brauer, A., [1] Über einige spezielle diophantische Gleichungen, *Math. Z.* **25** (1926) 499–504.

[2] On a property of k consecutive integers, *Bull. Amer. Math. Soc.* **47** (1941) 328–331.

Brauer, A. and Reynolds, R.L., [1] On a theorem of Aubry-Thue, *Canadian J. Math.* **3.** (1951) 367–374.

Bredihin, B.M., [1] Binary additive problems of indeterminate type (in Russian) I, II, *Izv. Akad. Nauk. SSSR, Ser. mat.* **27** (1963) 439–462, 577–612.

Bremner, A., [1] Integer points on a special cubic surface, *Duke Math. J.* **44** (1977) 757–765.

Brent, R.P., [1] The first occurrence of large gaps between successive primes, *Math. Comp.* **27** (1973) 959–963.

[2] Irregularities of distribution of primes and twin primes, *Math. Comp.* **29** (1975) 43–56.

[3] Tables concerning irregularities in the distribution of primes and twin primes, deposited in the UMT file, cf. *Math. Comp.* **30** (1976) 379.

[4] The first occurrence of certain large prime gaps, *Math. Comp.* **35** (1980) 1435–1436.

Brillhart, J., Lehmer, D.H., Selfridge, J.L., Tuckerman, B., Wagstaff, S.S. Jr., [1] *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, (Providence 1983).

Brillhart, J., Tonascia, J. and Weinberger, P., [1] On the Fermat quotient, in: A.O.L. Atkin and B.J. Birch (eds.), *Computers in Number Theory*, 213–222 (London 1971).

Bromhead, T., [1] On square sums of squares, *Math. Gaz.* **44** (1960) 219–220.

Browkin, J., [1] Certain property of triangular numbers (in Polish), *Wiadom. Mat.* **2** (1957–59) 253–255.

[2] Solution of a certain problem of A. Schinzel (in Polish), *Prace Mat.* **3** (1959) 205–207.

Brown, A.L., [1] Multiperfect numbers, *Scripta Math.* **20** (1954) 103–106.

[2] Multiperfect numbers — Cousins of the perfect numbers — No. 1, *Recreational Math. Mag.* 14 (1964) 31–39.

Brown, J.L. Jr., [1] On Lamé's Theorem, *Fibon. Quart.* **5** (1967) 153–160.

[2] Generalization of Richert's theorem, *Amer. Math. Monthly* **83** (1976) 631–634.

Brun, V., [1] La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\dots$ où les dénominateurs sont „nombres premiers jumeaux" est convergente ou finie, *Bull. Sci. Math.* **43** (1919) 100–104, 124–128.

[2] Le crible d'Eratosthène et le théorème de Goldbach, *Vid.Selsk.Skr.* I *Math.Nat.Kl.* Kristiania 1920, No. 3.

Buck, R.C., [1] Prime representing functions, *Amer. Math. Monthly* **53** (1946) 265.

Buhler, J.P., Crandall, R.E. and Penk, M.A., [1]. Primes of the form $n! \pm 1$ and $2 \cdot 3 \cdot 5 \dots p \pm 1$, *Math. Comp.* **38** (1982) 639–643, Corrigendum *ibid.* **40** (1983) 72.

Buxton, M. and Elmore, S., [1] An extension of lower bounds for odd perfect numbers, *Notices Amer. Math. Soc.* **23** (1976), A-55.

Cantor, G., [1] Ueber die einfachen Zahlensysteme, *Zeitschr. Math. Phys.* **14** (1869) 121–128.

[2] Zwei Sätze über eine gewisse Zerlegung der Zahlen in unendliche Produkte, *Zeitschr. Math. Phys.* **14** (1869) 152–158.

Carmichael, R.D., [1] On Euler's φ-function, *Bull. Amer. Math. Soc.* **13** (1907), 241–243 and Errata, *ibidem* **54** (1948) 1192.

[2] Note of a new number theory function, *Bull. Amer. Math. Soc.* **16** (1910) 232–238.

[3] On composite numbers P, which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, *Amer. Math. Monthly* **19** (1912) 22–27.

[4] *Diophantine Analysis* (New York 1915, reprint New York 1959).

[5] Note on Euler's φ-function, *Bull. Amer. Math. Soc.* **28** (1922) 109–110.

Cassels, J.W.S., [1] The rational solutions of the Diophantine equation $Y^2 = X^3 - D$, *Acta Math.* **82** (1950) 243–273.

[2] The rational solutions of the Diophantine equation $Y^2 = X^3 - D$, Addenda and Corrigenda, *Acta Math.* **84** (1951) 299.

[3] On the equation $a^x - b^y = 1$, II, *Proc. Cambridge Philos. Soc.* **56** (1960) 97–103, Corrigendum, *ibidem* **57** (1961) 187.

[4] On a Diophantine equation, *Acta Arith.* **6** (1960) 47–52.

Cattaneo, P., [1] Sui numeri quasiperfetti, *Boll. Un. Mat. Ital.* (3) **6** (1951) 59–62.

Cel, J., [1] On decomposition of a cube into the difference of two biquadrates (in Polish), *Matematyka* **36** (1983) 308–310.

Chakrabarti, M.C., [1] On the limit points of a function connected with the three-square problem, *Bull. Calcutta Math. Soc.* **32** (1940) 1–6.

Champernowne, G.D., [1] Construction of decimals normal in the scale of ten, *J. London Math. Soc.* **8** (1933) 254–260.

Chein, E. Z., [1] Some remarks on the exponential Diophantine equation, *Notices Amer. Math. Soc.*, **26** (1979) A-426.

[2] Remark on the binomial coefficients, *Notices Amer. Math. Soc.* **26** (1979) A-506.

Chen, J. R., [1] Waring's problem for $g(5)$, *Sc. Sinica* **12** (1964), 1547–1568.

[2] On the representation of a large even number as the sum of a prime and the product of at most two primes, *Sc. Sinica* **16** (1973) 157–176.

[3] On the least prime in an arithmetical progression and theorems concerning the zeros of Dirichlet's L functions, *Sci. Sinica* **22** (1979) 859–889.

Chernick, J., [1] On Fermat's simple theorem, *Bull. Amer. Math. Soc.* **45** (1939) 269–274.

Chikawa, K., Isêki, K. and Kusakabe, T., [1] On a problem by H. Steinhaus, *Acta Arith.* **7** (1962) 251–252.

Chikawa, K., Isèki, K., Kusakabe, T. and Shibamura, K., [1] Computation of cyclic parts of Steinhaus problem for power 5, *Acta Arith.* **7** (1962) 253–254 and Corrigendum, *ibid.* **8** (1963) 259.

Choi, S.L.G., [1] Covering the set of integers by congruence classes of distinct moduli, *Math. Comp.* **25** (1971) 885–895.

Chojnacka-Pniewska, M., [1] Sur les congruences aux racines données, *Ann. Polon. Math.* **3** (1956) 9–12.

Chowla, S., [1] An extension of Heilbronn's class-number theorem. *Quart. J. Math. Oxford Ser.* **5** (1934), 304–307.

[2] There exists an infinity of 3-combinations of primes in A.P., *Proc. Lahore Philos. Ser.* **6**, no 2 (1944) 15–16.

Chowla, S. and Briggs, W.E., [1] On discriminants of binary quadratic forms with a single class in each genus, *Canadian J. Math.* **6** (1954) 463–470.

Cipolla, M., [1] Sui numeri composti P, che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \bmod P$, *Ann. Mat. Pura Appl.* (3) **9** (1903) 139–160.

Clement, P.A., [1] Congruences for sets of primes, *Amer. Math. Monthly* **56** (1949) 23–25.

[2] Representation of integers in the form: a k-th power plus a prime, *Amer. Math. Monthly* **56** (1949) 561.

Coblyn, [1] Sur les couples de nombres premiers, *Soc. Math. de France, C.R. des Séances* **55** (1913), 55–57.

Coghlan, F.B., and Stephens, N. M., [1] The diophantine equation $x^3-y^2=k$, in: A. O. L. Atkin and B.J. Birch (eds), *Computers in number theory*, 199–205 (London 1971).

Cohen, E., [1] Arithmetical notes. V. A divisibility property of the divisor function, *Amer. J. Math.* **83** (1961) 693–697.

Cohen, G.L. and Hagis, P. Jr., [1] On the number of prime factors of n if $\varphi(n) \mid n-1$, *Nieuw Arch. Wisk.* (3) **28** (1980) 177–185.

Cohen, H., [1] On amicable and sociable numbers, *Math. Comp.* **24** (1970) 423–429.

Colombo, M., [1] Tavole numeriche e diagrammi sulla distribuzione delle coppie di numeri primi a differenza fissa, *Ist. Lombardo Sci. Lett. Rend. A* **93** (1959) 95–133.

de Comberousse, C., [1] Algèbre supérieure **1** (Paris 1887).

Copeland, A. and Erdös, P., [1] Note on normal numbers, *Bull. Amer. Math. Soc.*, **52** (1946) 857–860.

Cormack, G.V. and Williams, H.C. [1] Some very large primes of the form $k \cdot 2^n + 1$, *Math. Comp.* **35** (1980) 1419–1421.

van der Corput, J.G., [1] Sur l'hypothèse de Goldbach pour presque tous les nombres pairs, *Acta Arith.* **2** (1937) 266–290.

[2] Über Summen von Primzahlen und Primzahlquadraten, *Math. Ann.* **116** (1939) 1–50.

[3] On de Polignac's conjecture (in Dutch), *Simon Stevin* **27** (1950) 99–105.

Coustal, R., [1] Calcul de $\sqrt{2}$, et reflexion sur une espérance mathématique, *C.R. Acad. Sci. Paris* **230** (1950) 431–432.

Cramér, H., [1] On the order of magnitude of the difference between consecutive prime numbers, *Acta Arith.* **2** (1936) 396–403.

Crocker, R., [1] A theorem concerning prime numbers, *Math. Mag.* **34** (1960/61) 316, 344.

[2] On the sum of a prime and of two powers of two, *Pacific J. Math.* **36** (1971) 103–107.

Cunningham, A.J.C. and Woodall, H.J., [1] Factorization of $Q = (2^q \pm q)$ and $(q^{2^q} \pm 1)$, *Messenger Math.* **47** (1917) 1–38.

Danilov, L.V., [1] Letter to the editors (in Russian) *Mat. Zam.* **36** (1984) 457–459.

Davenport, H., [1] On Waring's problem for fourth powers, *Ann. of Math.* (2) **40** (1939) 731–747.

[2] *The Higher Arithmetic, An Introduction to the Theory of Numbers* (London and New York 1952, fifth ed. Cambridge 1982).

Dem'yanenko, V.A., [1] On Jeśmanowicz problem for Pythagorean numbers (in Russian), *Izv. Vyssh. Uchebn. Zaved. Matematika* 1965, no **5** (48) 52–56.

[2] Sums of four cubes (in Russian), *Izv. Vyssh. Uchebn. Zaved. Matematika* 1966, no **5** (54) 64–69.

[3] On a conjecture of A. Schinzel (in Russian), *Izv. Vyssh. Uchebn. Zaved. Matematika* 1975, no **8** (159) 33–45.

[4] On a conjecture of A. Mąkowski (in Russian), *Izv. Vyssh. Uchebn. Zaved. Matematika* 1976, no **10** (173) 29–31.

Dénes, P., [1] Über die Diophantische Gleichung $x^l + y^l = cz^l$, *Acta Math.* **88** (1952) 212–251.

Depman, I.Ya., [1] The notable Slavic computers G. Vega and Ya. F. Kulik (in Russian), *Istor.-Mat. Issled.* **6** (1953) 593–604.

Desboves, A., [1] Sur un théorème de Legendre et son application à la recherche de limites qui comprennent entre elles des nombres premiers, *Nouv. Ann. Math.* **14** (1855) 281–295.

Devitt, J.S. [1] Aliquot sequences, MSc. thesis, The Univ. of Calgary 1976, cf. *Math. Comp.* **32** (1978) 942–943.

Dickson, L.E., [1] A new extension of Dirichlet's theorem on prime numbers, *Messenger Math.* **33** (1904) 155–161.

[2] Amicable number triples, *Amer. Math. Monthly* **20** (1913) 84–91.

[3] Theorems and tables on the sum of the divisors of a number, *Quart. J. Pure Appl. Math.* **44** (1913) 264–296.

[4] Proof of the ideal Waring theorem for exponents 7-180, *Amer. J. Math.* **58** (1936) 521-529.

[5] Solution of Waring's problem, *Amer. J. Math.* **58** (1936) 530-535.

[6] *Modern Elementary Theory of Numbers* (Chicago 1939).

[7] *History of the Theory of Numbers*, 3 vols. (Washington 1919-1923, reprint New York 1966)

Dirichlet, P.G.L., [1] Sur l'équation $t^2+u^2+v^2+w^2 = 4m$, *J. Math. Pures Appl.* (2) **1** (1856) 210-214.

Dixon, J.D., [1] The numbers of steps in the Euclidean algorithm. *J. Number Theory* **2** (1970) 414-422.

[2] A simple estimate for the number of steps in the Euclidean algorithm, *Amer. Math. Monthly* **78** (1971) 374-376.

Dress, F., [1] Amélioration de la majoration de $g(4)$ dans le problème de Waring: $g(4) \leqslant 30$, *Acta Arith.* **22** (1973) 173-147

Dressler, R.E., Mąkowski, A. and Parker, T., [1] Sums of distinct primes from congruence classes modulo 12, *Math. Comp.* **28** (1974) 651-652.

Duparc, H.J.A., [1] On Carmichael numbers, *Simon Stevin* **39** (1952) 21-24.

[2] On Mersenne numbers and Poulet numbers, Math. Centrum Amsterdam, Rapport ZW 1953 — 001 (1953).

Dutka, J., [1] The square root of 2 to 1000000 decimals, *Math. Comp.* **25** (1971) 927-930.

Dyer-Bennet, J., [1] A theorem on partitions of the set of positive integers, *Amer. Math. Monthly* **47** (1940) 152-154.

Editorial Note, [1] Editorial Note, *Math. Comp.* **15** (1961) 82.

Erdös, P., [1] Beweis eines Satzes von Tschebyschef, *Acta Litt. Sci. Szeged* **5** (1932) 194-198.

[2] A theorem of Sylvester and Schur, *J. London Math. Soc.* **9** (1934) 282-288.

[3] On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function, *Quart. J. Math. Oxford Ser.* **6** (1935) 205-213.

[4] On the sum and difference of squares of primes, *J. London Math. Soc.* **12** (1937) 133-136, 168-171.

[5] Note on products of consecutive integers, *J. London Math. Soc.* **14** (1939) 194-198.

[6] Integral distances, *Bull. Amer. Math. Soc.* **51** (1945) 996.

[7] On some applications of Brun's method, *Acta Univ. Szeged Sect. Sci. Math.* **13** (1949) 57-63.

[8] On the converse of Fermat's theorem, *Amer. Math. Monthly* **56** (1949) 623-624.

[9] On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, *Proc. Nat. Acad. Sci. U.S.A.* **35** (1949) 374-384.

[10] On integers of the form 2^k+p and some related problems, *Summa Brasil. Math.* **2** (1950) 113-123.

[11] On a Diophantine equation, *J. London Math. Soc.* **26** (1951) 176-178.

[12] On consecutive integers, *Nieuw Arch. Wisk.* (3) **3** (1955) 124-128.

[13] On amicable numbers, *Publ. Math. Debrecen* **4** (1955) 108-111.

[14] Some remarks on Euler's φ function, *Acta Arith.* **4** (1958) 10-19.

[15] Solution of two problems of Jankowska, *Bull. Acad. Polon Sci. Sér. Sci. Math. Astr. Phys.* **6** (1958) 545-547.

[16] Some remarks on the functions φ and σ, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys.* **10** (1962) 617-619.

[17] Über die Zahlen der Form $\sigma(n)-n$ und $n-\varphi(n)$, *Elem. Math.* **28** (1973) 83–86.

Erdös, P. and Mirsky, L., [1] The distribution of values of the divisor function $d(n)$, *Proc. London Math. Soc.* (3) **2** (1952) 257–271.

Erdös, P. and Obláth, R., [1] Über diophantische Gleichungen der Form $n! = x^p \pm y^p$ und $n! \pm m! = x^p$, *Acta Litt. Sci. Szeged* **8** (1936) 241–255.

Erdös, P. and Rényi, A., [1] Some problems and results on consecutive primes, *Simon Stevin* **27** (1950) 115–125.

Erdös, P. and Schinzel, A., [1] Distributions of the values of some arithmetical functions, *Acta Arith.* **6** (1961) 473–485.

Erdös, P. and Selfridge, J.L., [1] The product of consecutive integers is never a power. *Illinois J. Math.* **19** (1975) 292–301.

Erdös, P. and Turán, P., [1] On some sequences of integers, *J. London Math. Soc.* **11** (1936) 261–264.

[2] On some new questions on the distribution of prime numbers, *Bull. Amer. Math. Soc.* **54** (1948) 371–378.

Estermann, T., [1] Einige Sätze über quadratfreie Zahlen, *Math. Ann.* **105** (1931) 653–662.

[2] Note on a paper of A. Rotkiewicz, *Acta Arith.* **8** (1963) 465–467.

Faber, G., [1] Über die Abzählbarkeit der rationalen Zahlen, *Math. Ann.* **60** (1905) 196–203.

Fermat, P., [1] *Oeuvres*, vol. II (Paris 1894).

Finsler, P., [1] Über die Primzahlen zwischen n und $2n$, *Festschrift zum* 60. *Geburtstag von Prof. Dr Andreas Speiser*, 118–122 (Zürich 1945).

Franqui, B., and Garcia, M., [1] Some new multiply perfect numbers, *Amer. Math. Monthly* **60** (1953) 459–462.

[2] 57 new multiply perfect numbers, *Scripta Math.* **20** (1954) 169–171.

Fredericksen, H., [1] Schur numbers and the Ramsey number $N(3, 3, \ldots 3; 2)$, *J. Combin. Theory, Ser. A.* **27** (1979) 376–377.

Frobenius, G., [1] Über quadratische Formen, die viele Primzahlen darstellen, *S. Ber. Preuss. Akad. Wiss. Phys. Math. Kl.* 1912, 966–980.

Fröberg, C.E., [1] Some Computations of Wilson and Fermat Remainders, *Math. Tables Aids Comp.* **12** (1958) 281.

[2] Investigation of the Wilson remainders in the interval $3 \leqslant p \leqslant 50\,000$, *Ark. Mat.* **4** (1963) 479–499.

Früchtl, K., [1] Statistische Untersuchung über die Verteilung von Primzahl-Zwillingen, *Anz. Öster. Akad. Wiss. Math. Nat. Kl.* **87** (1950) 226–232.

Fueter, R., [1] Über kubische diophantische Gleichungen, *Comment. Math. Helv.* **2** (1930) 69–89.

Gabard, E., [1] Factorisations et équation de Pell, *Mathesi* **67** (1958) 218–220.

Gabowicz, J.A., [1] Solutions of the equation $x^3+y^3+z^3-t^3 = 1$ in natural numbers (in Polish), *Wiadom. Mat.* 7 (1963) 63–64.

Gardiner, V.L., Lazarus, R.B. and Stein, P.R., [1] Solutions of the diophantine equation $x^3+y^3 = z^3-d$, *Math. Comp.* **18** (1964) 408–413.

Gasper, R.W Jr., [1] Table of simple continued fractions for π and the derived decimal approximation, deposited in the UMT file, cf. *Math. Comp.* **31** (1977) 1044.

Gelfond, A.O., [1] A common property of number systems (in Russian), *Izv. Akad. Nauk SSSR, Ser. Mat.* **23** (1959) 809–814.

Georgiev, G., [1] On the solution in rational numbers of certain diophantine equations (in Polish), *Prace Mat.* **1** (1955) 201–238.

Gerono, C.G., [1] Note sur la résolution en nombres entiers et positifs de l'équation $x^m = y^n + 1$, *Nouv. Ann. Math.* (2) **9** (1870) 469–471, **10** (1871) 204–206.

Gilloud, J. and Bourger, M., [1] *Un million de décimals de* π (Paris 1974)

Ginsburg., J., [1] The generators of a Pythagorean triangle, *Scripta Math.* **11** (1945) 188.

Giuga, G., [1] Su una presumabile proprietà caratteristica dei numeri primi, *Ist. Lombardo Sci. Lett. Rend., Cl. Sci. Mat. Nat.* (3) **14** (1950) 511–528.

Glaisher, J.W.L., [1] Mathematical notes 1. An arithmetical proposition, *Messenger of Math.* (2) **2** (1873) 41–43.

[2] *Number Divisor Tables* (Cambridge 1940).

Godwin, H.J., [1] A note $x^3+y^3+z^3 = 1$, J. *London Math. Soc.* **32** (1957) 501–503.

Golomb, S., [1] Sets of primes with intermediate density, *Math. Scand.* 3 (1955) 264–274.

Golubew, W.A., [1] Abzählung von „Vierlingen" von 2000000 bis 3000000 und von „Fünflingen" von 0 bis 2000000, *Anz. Österr. Akad. Wiss. Math. Nat. Kl.* **93** (1956) 153–157.

[2] Abzählung von „Vierlingen" und „Fünflingen" bis zu 5000000 und von „Sechslingen" von 0 bis 14000000, *Anz. Österr. Akad. Wiss. Math Nat. Kl.* **94** (1957) 82–87.

[3] Abzählung von „Vierlingen" und „Fünflingen" bis zu 10000000, Einige Formeln, *Anz. Österr. Akad. Wiss. Math. Nat. Kl.* **94** (1957) 274–280.

[4] Abzählung von „Vierlingen" und „Fünflingen" bis zu 15000000, *Anz. Österr. Wiss. Math. Nat. Kl.* **96** (1959) 227–232.

[5] Primzahlen der Form x^2+1, *Anz. Österr. Akad. Wiss. Math. Nat. Kl.* **95** (1958) 9–13; **96** (1959) 126–129; **97** (1960) 39–44, 312–319; **98** (1961) 59–63; **99** (1962) 33–37.

[6] Primzahlen der Form x^2+7, *Anz. Österr. Akad. Wiss. Math. Nat. Kl.* **98** (1961) 165–169; **100** (1963) 244–251.

Goodstein E., [1] A note on magic squares, *Math. Gaz.* **24** (1940) 117.

Graham, S., [1] On Linnik's constant, *Acta Arith.* **39** (1981) 163–179.

Grosswald, E., [1] Negative discriminants of binary quadratic forms with one class in each gems, *Acta Arith.* 8 (1963) 295–306.

[2] *Representation of integers as sums of squares* (New York 1985).

Grosswald, E., Calloway, A., and Calloway, J., [1] The representation of integers by three positive squares, *Proc. Amer. Math. Soc.* **10** (1959) 451–455.

Grosswald, E. and Hagis, P., Jr., [1] Arithmetic progressions consisting only of primes, *Math. Comp.* 33 (1979) 1343–1352.

Grube, F., [1] Ueber Einige Euler'sche Sätze aus der Theorie der quadratischen Formen, *Zeitschr. Math. Phys.* **90** (1874) 492–519.

Gupta, H., [1] Congruence properties of $\sigma(n)$, *Math. Student* 13 (1945) 25–29.

[2] A table of values of $N_2(t)$, *Res. Bull. East Penjab Univ.* 1952 no. **20**, 13–93.

Guy, R.K. [1] *Unsolved Problems in Number Theory* (New York–Heidelberg–Berlin 1981).

Guy, R.K. and Shanks, D., [1] A constructed solution of $\sigma(n) = \sigma(n+1)$, *Fibon. Quart.* **12** (1974) 299.

Hadwiger, H., [1] Ungelöste Probleme Nr 24, *Elem. Math.* 13 (1958) 85.

Hagis, P., Jr., [1] A lower bound for the set of odd perfect numbers, *Math. Comp.* **27** (1973) 951–953.

[2] Outline of a proof that every odd perfect number has at least eight prime factors, *Math. Comp.* **34** (1980) 1027–1032.

HAGIS, P., Jr., and COHEN, G.L., [1] Some results concerning quasiperfect numbers, *J. Austral. Math. Soc.* **33** (1982) 275-286.

HALL, M., Jr., [1] On the sum and product of continued fractions *Ann. of Math.* (2) **48** (1947) 966-993.

[2] Cyclic projective planes, *Duke Math., J.* **4** (1947) 1079-1090.

[3] The Diophantine equation $x^3 - y^2 = k$, in: A. O. L. Atkin and B. J. Birek (eds.). *Computer in Number Theory*, 173-198 (London 1971).

HALTER-KOCH, F., [1] Darstellung natürlicher Zahlen als Summe von Quadraten, *Acta Arith.* **42** (1982) 11-20.

HANLY, V.S., [1] A proposition equivalent to Dirichlet's theorem, *Amer. Math. Monthly* **64** (1957) 742.

HARDY, G.H. and WRIGHT, E.M., [1] *An Introduction to the Theory of Numbers* (Oxford 1954)

HARRIS, V.C., [1] A modification of the sieve of Eratosthenes, *Amer. Math. Monthly* **60** (1953) 325-326.

HASSE, H., [1] *Vorlesungen über Zahlentheorie* (Berlin-Göttingen-Heidelberg 1950)

[2] Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verall meinerung, *Nagoya Math. J.* **27** (1966) 77-102.

HAUSDORFF, F., [1] *Grundzüge der Mengenlehre* (Leipzig 1914)

HAUSSNER, R., [1] Über die Verteilung von Lücken und Primzahlen, *J. Reine Angew. Math.* **168** (1932) 192.

HEATH-BROWN, D.R., [1] The divisior function at consecutive integers. *Mathematika* **31** (1984) 141-149.

HECKE, E., [1] Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen II, *Math. Z.* **6** (1920) 11-51.

HEMER, O., [1] *On the Diophantine Equation* $y^2 - k = x^3$, Diss. (Upsala 1952).

[2] Note on the Diophantine equation $y^2 - k = x^3$, *Ark. Mat.* **3** (1954) 67-77.

HENSEL, K., [1] Ueber den grössten gemeinsamen Theiler aller Zahlen, welche durch eine ganze Function von n Veränderlichen darstellbar sind, *J. Reine. Angew. Math.* **116** (1896) 350-356.

HENSLEY, D. and RICHARDS, I., [1] Primes in intervals, *Acta Arith.* **25** (1974) 375-391.

HILL, J.D., [1] Solution of the problem 3449, *Amer. Math. Monthly* **38** (1931) 298-299.

HORNFECK, B. und WIRSING, E., [1] Über die Häufigkeit vollkommener Zahlen, *Math. Ann.* **133** (1957) 431-438.

HOOLEY, C., [1] On the power-free values of polynomials, *Mathematika* **14** (1967) 21-26.

HUNSUCKER, J.L., NEBB, J. and STARNS, R.E., [1] Computational results concerning some equations involving $\sigma(n)$, *Math. Student* **41** (1973) 285-289.

HURWITZ, A., [1] Über eine besondere Art der Kettenbruch-Entwicklung reeller Grössen, *Acta Math.* **12** (1889) 367-405.

[2] Somme de trois carrés, *Intermédiaire Math.* **14** (1907) 106-107.

HYYRÖ, S., [1] On the Catalan problem (in Finnish), *Archimedes* **1** (1963) 53-54.

IRVING, R.W., [1] An extension of Schur's theorem on sum-free partitions, *Acta Arith.* **25** (1973) 55-63.

ISÉKI, K., [1] A problem of number theory, *Proc. Japan Acad.* **36** (1960) 578-583.

[2] Necessary results for computation of cyclic parts in Steinhaus problem, *Proc. Japan Acad.* **36** (1960) 650-651.

ISÉKI, K. and TAKADA, I., [1] On Steinhaus problem in number theory, Computation of cyclic parts of Steinhaus problem for power 9, *Mathem. Seminar Notes Kobe Univ.* **8** (1980) 227 231.

IVIĆ A., [1] *The Riemann Zeta-Function, the Theory of the Riemann Zeta-Function with Applications* (New York-Chichester-Brisbane-Toronto-Singapore 1985).

IWANIEC, H., [1] Almost primes represented by quadratic polynomials, *Invent. Math.* **47** (1978) 171-188.

JACOBI, C., [1] De compositione numerorum ex quatuor quadratis, *J. Reine Angew. Math.* 12 (1834) 167-172.

JAESCHKE, G., [1] On the smallest k such that all $k \cdot 2^n + 1$ are composite, *Math. Comp.* **40** (1983) 381-384.

JAKÓBCZYK, F., [1] Les applications de la fonction $\lambda_g(n)$ à l'étude des fractions périodiques et de la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$, *Ann. Univ. Mariae Curie-Skłodowska, Sect. A*, **5** (1951) 97-138.

JANKOWSKA, S., [1] Les solutions du système d'équations $\varphi(x) = \varphi(y)$ et $\sigma(x) = \sigma(y)$ pour $x < y < 10000$, *Bull. Acad. Polon. Sci. Sér Sc. Math. Astr. Phys.* **6** (1958) 541-543.

JEŚMANOWICZ, L., [1] Several remarks on Pythagorean triangles (in Polish), *Wiadom. Mat.* 1 (1956) 196-202,

de JONCOURT, E., [1] *De Natura et Praeclaro Usu Simplicissimae Speciei Numerorum Trigonalium* (Hagae 1762).

JONES, B.W. and PALL, G., [1] Regular and semiregular positive ternary quadratic forms. *Acta Math.* **70** (1939) 165-191.

JORDAN, C., [1] *Traité des substitutions* (Paris 1870).

JÓZEFIAK, T., [1] A curiosity concerning triangular numbers (in Polish), *Matematyka* 13 (1960) 327.

[2] On a hypothesis of L. Jeśmanowicz concerning Pythagorean numbers (in Polish), *Prace Mat.* **5** (1961) 119-123.

KANOLD, H.J., [1] Untere Schranken für teilerfremde befreundete Zahlen, *Arch. Math.* **4** (1953) 399-401.

[2] Über zahlentheoretische Funktionen, *J. Reine Angew. Math.* **195** (1955) 180-191.

KELLER, W., [1] Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$, *Math. Comp.* 41 (1983) 661-673.

[2] New factors of Fermat numbers, *Abstracts Amer. Math. Soc.* **5** (1984) 391-392.

[3] The 17th prime of the form $5 \cdot 2^n + 1$, *Abstracts Amer. Math. Soc.* **6** (1985) 31.

KHATRI, M.N., [1] Triangular numbers and Pythagorean triangles, *Scripta Math.* 21 (1955) 94.

KHINCHIN, A.Ya., [1] *Three Pearls of Number Theory* (Rochester 1952)

KILLGROVE, R.B. and RALSTON, K.E., [1] On a conjecture concerning primes, *Math. Tables Aids Comp.* 13 (1959) 121-122.

KLEE, V.L. Jr., [1] On the equation $\varphi(x) = 2m$, *Amer. Math. Monthly* **53** (1946) 327-328.

[2] Some remarks on Euler's totient, *Amer. Math. Monthly* **54** (1947) 332.

[3] A generalization of Euler's φ function, *Amer. Math. Monthly* **55** (1948) 358-359.

KNÖDEL, W., [1] Carmichaelsche Zahlen, *Math. Nachr.* **9** (1953) 343-350.

KOGBETLIANZ, E. and KRIKORIAN, A., [1] *Handbook of First Complex Prime Numbers, Part 2, Tables of Decompositions of Real Primes of Type* $4N+1$ *into Sums of two Squares* (London-New York-Paris 1971).

Ko Chao, [1] Note on the Diophantine equation $x^x y^y = z^z$, *J. Chinese Math. Soc.* **2** (1940) 205-207.

[2] Remark on Pythagorean numbers (in Chinese), *Acta Sc. Nat. Univ. Szechuan*, 1958, 73-80.

[3] On a conjecture of Jeśmanowicz (in Chinese), *Acta Sc. Nat. Univ. Szechuan*, 1958, 81-90.

[4] On a Diophantine equation $(a^2-b^2)^x+(2ab)^y = (a^2+b^2)^z$ (in Chinese), *Acta Sc. Nat. Univ. Szechuan*, 1959, 25-34.

Kolesnik, G., [1] On the method of exponent pairs, *Acta Arith.* **45** (1985) 115-143.

Korec, I., [1] Nonexistence of small perfect rational cuboid, II *Acta Math. Univ. Comen.* **44-45** (1984) 39-48.

Korhonen, O., [1] On the diophantine equation $Ax^2+2B = y^n$, *Acta Univ. Duluensis, Ser. A, Math.* **No** 17 (1979).

Kraïtchik. M., [1] *Théorie des nombres* II (Paris 1926).

[2] *Recherches sur la Théorie des Nombres* II, *Factorisation* (Paris 1929).

[3] *Théorie des nombres* III. *Analyse diophantienne et applications aux cuboïdes rationnels* (Paris 1947).

[4] *Introduction à la Théorie des Nombres* (Paris 1952).

Krishnawami, A.A., [1] On isoperimetrical Pythagorean triangles, *Tôhoku Math. J.* **27** (1926) 332-348.

Kulik, J.Ph., Poletti, L. et Porter, R.J., [1] *Liste des nombres premiers du onzième million (plus précisément de* 100006741 *à* 10999997) *d'après des tables manuscrites* (Amsterdam 1951)

Kulikowski, T., [1] Sur l'existence d'une sphère passant par un nombre donné de points aux coordonnées entières, *Enseignement Math.* (2) **5** (1959) 89-90.

Lagarias, J.C., Miller, V.S. and Odlyzko A.M., [1] Computing $\pi(x)$: The Meissel-Lehmer method, *Math. Comp.* **44** (1985) 537-560.

Lagrange, J., [1] Sets of n squares of which any $n-1$ have their sum square, *Math. Comp.* **41** (1983) 675-681.

Lal, M. and Gillard, P., [1] On the equation $\phi(n) = \phi(n+k)$, *Math. Comp.* **25** (1972) 579-583.

Lal, M., Russell, W. and Blundon, W.J., [1] A note on sums of four cubes, *Math. Comp.* **23** (1969) 423-424.

Lamé, G., [1] Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers, *C.R. Acad. Sci. Paris* **19** (1844) 867-870.

Landau, E., [1] Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, *Arch. Math. Phys.* (3) 13 (1908) 305-312.

[2] *Vorlesungen über Zahlentheorie*, 3 vols (Leipzig 1927, reprint New York 1947).

[3] *Handbuch der Lehre von der Verteilung der Primzahlen*, 2 vols., 2nd ed. with an Appendix by P.T. Bateman (New York 1953)

Lander, L.J. and Parkin, T.R., [1] Equal sums of biquadrates, *Math. Comp.* **20** (1966) 450-451; Corrigendum, *ibid.* **21** (1967) 296.

[2] A counterexample to Euler's sum of powers conjecture, *Math. Comp.* 21 (1967) 101-103.

[3] On first appearance of prime difference, *Math. Comp.* **21** (1967) 483-488.

[4] Consecutive primes in arithmetic progression, *Math. Comp.* **21** (1967) 489.

Lander, L.J., Parkin, T.R. and Selfridge, J.L., [1] A survey of equal sums of like powers, *Math. Comp.* **21** (1967) 446–459.

Langevin, M., [1] Quelques applications de nouveaux résultats de van der Poorten, *Séminaire Delange-Pisot-Poitou* 17 (1975/76) No 12, 1–11.

Lebesgue, H., [1] Sur certaines démonstrations d'existence, *Bull. Soc. Math. France* **45** (1917) 132–144.

Lebesgue, V.A., [1] Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nouv. Ann. Math.* **9** (1850) 178–181.

[2] Note sur quelques équations indéterminées, *Nouv. Ann. Math.* (2) **8** (1869) 452–456, 559.

Lee, E.J., Madachy, J.S., [1] The history and discovery of amicable numbers, *J. Recreational Math.* **5** (1972) 77–93; 155–173; 231–249, Errata, *ibid.* **6** (1973) 164, 229.

Leech, J., [1] Note on the distribution of prime numbers, *J. London Math. Soc.* **32** (1957) 56–58.

[2] The rational cuboid revisited, *Amer. Math. Monthly* **84** (1977) 518–533, Corrections *ibid.* **85** (1978) 473.

Legendre, A.M., [1] *Essai sur la théorie des nombres* (Paris 1798).

Lehmer, D.H., [1] On Euler's totient function, *Bull. Amer. Math. Soc.* **38** (1932) 745–751.

[2] On Lucas's test for the primality of Mersenne's numbers, *J. London Math. Soc.* **10** (1935) 162–165.

[3] On the converse on Fermat's theorem, *Amer. Math. Monthly* **43** (1936) 347–354.

[4] On the partition of numbers into squares, *Amer. Math. Monthly* **55** (1948) 476–481.

[5] On a conjecture of Krishnaswami, *Bull. Amer. Math. Soc.* **54** (1948) 1185–1190.

[6] On the converse of Fermat's theorem II, *Amer. Math. Monthly* **56** (1949) 300–309.

[7] On the Diophantine equation $x^3 + y^3 + z^3 = 1$, *J. London Math. Soc.* 31 (1956) 275–282.

[8] On the exact number of primes less than a given limit, *Illinois J. Math.* 3 (1959) 381–388.

[9] On Fermat's quotient, base 2, *Math. Comp.* **36** (1981) 289–290.

Lehmer, D.N., [1] *Factor Table for the First Ten Millions Containing the Smallest Factor of Every Number not Divisible by* 2, 3, 5 *or* 7 *Between the Limits* 0 *and* 10017000 (Washington 1909, reprint New York 1956).

Lerch, M., [1] Zur Theorie der Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$, *Math. Ann.* **60** (1905) 471–490.

Leszczyński, B., [1] On the equation $n^x + (n+1)^y = (n+2)^z$ (in Polish), *Wiadom. Mat.* 3 (1959–60) 37–39.

Le Veque, W.J., [1] The distribution of values of multiplicative functions, *Michigan Math. J.* 2 (1953–54) 179–192.

[2] *Topics in Number Theory*, 2 vols. (Reading 1956).

Lietzmann, W., [1] *Lustiges und merkwürdiges von Zahlen und Formen* (Göttingen 1930).

Light, W.A., Forrest, J., Hammond, N. and Roe, S., [1] A note on Goldbach's conjecture, *Nordisk Tidskr. Informationsbehandling* (BIT) **20** (1980) 525.

Lind, C.E., [1] *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven von Geschlecht Eins*, Diss. (Uppsala 1940)

Lindenbaum, A., [1] Sur les ensembles dans lesquels toutes les équations d'une famille donnée ont un nombre de solutions fixé d'advance, *Fund. Math.* **20** (1933) 1–29.

LINNIK, YU.V., [1] On the representation of large numbers as sums of seven cubes, *Mat. Sb. N.S.* 12 (1943) 220-224.

[2] An elementary solution of the problem of Waring by the Schnirelman method (in Russian), *Mat. Sb. N. S.* 12 (1943) 225-230.

LIOUVILLE, J., [1] Sur l'équation $1 \cdot 2 \cdot 3 \ldots (p-1)+1 = p^m$, *J. Math. Pures Appl.* (2) 1 (1856) 351-352.

LITVER, E. L., YUDINA, G.E., [1] Primitive roots for the first million primes and their powers (in Russian), *Matematičeskij analiz i ego primienienija*, vol. 3, 106-109 (Rostov on Don 1971).

LJUNGGREN, W., [1] Zur Theorie der Gleichung $x^2+1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo* I, 1942, no 5.

[2] Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen, *Ark. Mat. Astr. Fys.* 39A no 13 (1943).

[3] On the Diophantine equation $x^2+p^2 = y^n$, *Norske Vid. Selsk. Forh.* (Trondheim) **16** (1943) 27-30.

[4] Solution complète de quelques équations du sixième degré à deux indéterminées, *Arch. Math. Naturvid.* **48** (1946) 177-212.

[5] New solution of a problem proposed by E. Lucas, *Norsk Mat. Tidsskr.* **34** (1952) 65-72.

LOCHS, G., [1] Die ersten 968 Kettenbruchnenner von π, *Monatsh. Math.* **67** (1963) 311-316.

LONDON, H. and FINKELSTEIN, R., [1] *On Mordell's Equation $y^2-k = x^3$* (Bowling Green, Ohio 1973)

LUCAS, E., [1] Question 1180, *Nouv. Ann. Math.* (2) 14 (1875) 336.

[2] *Théorie des nombres*, Vol. I (Paris 1891, reprint Paris 1961).

LU WEN-TWAN, [1] On Pythagorean numbers $4n^2-1$, $4n$, $4n^2+1$ (in Chinese), *Acta Sc. Nat. Univ. Szechuan* 1959, 39-42.

MAHLER, K., [1] On the fractional parts of the powers of a rational number (II), *Mathematika* 4 (1957) 122-124.

MAIER, H. and POMERANCE, C., [1] On the number of distinct values of Euler's ϕ-function, *Acta Arith.* **49** (to appear).

MAKNIS, M., [1] Density theorems for Mecke Z-functions and the distribution of the prime numbers of an imaginary quadratic field (in Russian), *Litovsk. Mat. Sb.* **16** (1976) no 1, 173-180.

MARGENSTERN, M., [1] Résultats et conjectures sur les nombres pratiques, *C. R. Acad. Sci. Paris, Sér.* I *Math.* **299** (1984) 895-898.

MASAI, P. and VALETTE, A. [1] A lower bound for a counterexample to Carmichael's conjecture, *Boll. Unione Mat. Ital.* (6) A1 (1982) 313-316.

MASON, Th.E., [1] On amicable numbers and their generalizations, *Amer. Math. Monthly* **28** (1921) 195-200.

MAYAH, B.H., [1] The second Goldbach conjecture revisited, *Nordisk Tidskr. Informationsbehandling* (BIT) **8** (1968) 128-133.

MĄKOWSKI, A., [1] Sur quelques problèmes concernant les sommes de quatre cubes, *Acta Arith.* **5** (1959) 121-123.

[2] Remark on a paper of Erdös and Turán, *J. London Math. Soc.* **34** (1959) 480.

[3] On an arithmetic function (in Polish), *Matematyka* **10** (1959) 145-147.

[4] On some equations involving functions $\varphi(n)$ and $\sigma(n)$, *Amer. Math. Monthly* **67** (1960), pp. 668-670; Correction, *ibidem* **68** (1961) 650.

[5] Remarques sur les fonctions $\Theta(n)$, $\varphi(n)$ et $\sigma(n)$, *Mathesis* **69** (1960) 302-303.

[6] Three consecutive integers cannot be powers, *Colloq. Math.* **9** (1962) 297.

[7] Generalization of Morrow's D numbers, *Simon Stevin* **36** (1962) 71.

[8] Remarques sur les carrés magiques, *Mathesis* **70** (1962) 17-19.

[9] Some equations involving the sum of divisors, *Elem. Math.* **34** (1979) 82.

MCCURLEY, K.S., [1] An effective seven cube theorem, *J. Number Theory* **19** (1984) 176-183.

MELNIKOV, I.G., [1] La découverte des "nombres commodes" par Euler (in Russian) *Ist. Mat. Issled.* **13** (1960) 187-216.

MEYL, A., [1] Question 1194, *Nouv. Ann. Math.* (2) **17** (1878) 464-467.

MIENTKA, W.E. and VOGT, R.L. [1] Computational results relating to problems concerning $\sigma(n)$, *Mat. Vestnik* 7 (1970) 35-36.

MOESSNER, A., [1] A magic square of triangular numbers, *Math. Student* **10** (1942-43) 95.

[2] Magic squares, *Math. Student* **19** (1951) 124-126.

[3] All-prime magic squares, *Scripta Math.* **18** (1953) 303.

MORDELL, L.J., [1] The Diophantine equation $y^2-k=x^3$, *Proc. London Math. Soc.* (2) **13** (1913) 60-80.

[2] Note on the integer solutions of the equation $Ey^2=Ax^3+Bx^2+Cx+D$, *Messenger of Math.* **51** (1922) 169-171.

[3] On the four integer cubes problem, *J. London Math. Soc.* **11** (1936) 208-218, Addendum, *ibidem* **12** (1937) 80, and Corrigendum, *ibidem* **32** (1957) 383.

[4] On sums of three cubes, *J. London Math. Soc.* **17** (1942) 139-144.

[5] On the integer solutions of the equation $x^2+y^2+z^2+2xyz=n$, *J. London Math. Soc.* **28** (1953) 500-510 and Corrigendum, *ibidem* **32** (1957) 383.

[6] On intervals containing an affinely equivalent set of n integers mod k, *Proc. Amer. Math. Soc.* **5** (1954) 854-859.

[7] On the representation of a number as a sum of three squares, *Rev. Math. Pures Appl.* 3 (1958) 25-27.

MORET-BLANC, [1] Question 1175, *Nouv. Ann. Math.* (2) **15** (1876) 44-46.

MORROW, D.C., [1] Some properties of D numbers, *Amer. Math. Monthly* **58** (1951) 329-330.

MOSER, L., [1] Some equations involving Euler's totient function, *Amer. Math. Monthly* **56** (1949) 22-23.

[2] On the Diophantine equation $1^n+2^n+\dots+(m-1)^n=m^n$, *Scripta Math.* **19** (1953) 84-88.

[3] On non-averaging sets of integers, *Canadian J. Math.* **5** (1953) 245-252.

[4] On the theorems of Wilson and Fermat, *Scripta Math.* **22** (1957) 288.

MÜLLER, M., [1] Über die Approximation reeller Zahlen durch die Näherungsbrüche ihres regelmässigen Kettenbruches, *Arch. Math.* **6** (1955) 253-258.

NAGELL, T., [1] Zur Arithmetik der Polynome, *Abh. Math. Sem. Univ. Hamburg* **1** (1922) 184-188.

[2] Sur l'impossibilité de quelques équations à deux indéterminées. *Norsk Mat. Forenings Skrifter* **1** Nr 13 (1923).

[3] Einige Gleichungen von der Form $ay^2+by+c=dx^3$, *Norske Vid. Akad. Skrifter, Oslo* I, 1930, no 7.

[4] Solved problems (in Norwegian) *Norsk Mat. Tidsskr.* **30** (1948) 60–64.

[5] *Introduction to the Number Theory* (New York and Stockholm 1951, reprint 1964).

[6] Sur un théorème d'Axel Thue, *Ark. Mat.* **1** (1951) 489–496.

[7] On a special class of Diophantine equations of the second degree, *Ark. Mat.* 3 (1954) 51–65.

[8] Verallgemeinerung eines Fermatschen Satzes, *Arch. Math.* **5** (1954) 153–159.

[9] Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Soc. Sci. Upsal.* (4) **16** (1954) no 2.

[10] On the Diophantine equation $x^2+8D = y^n$, *Ark. Mat.* 3 (1954) 103–112.

[11] Sur une classe d'équations exponentielles, *Ark. Mat.* 3 (1958) 569–582.

[12] The diophantine equation $x^2+7 = 2^n$, *Ark. Mat.* 4 (1961) 182–185.

Niewiadomski, R., [1] Question 4202, *Intermédiaire Math.* **20** (1913) 78.

Obláth, R., [1] Une propriété des puissances parfaites, *Mathesis* **65** (1956) 356–364.

O'Keefe, E.S., [1] Verification of a conjecture of Th. Skolem., *Math. Scand.* **9** (1961) 80–82.

Ore, O., [1] *Number Theory and its History* (New York 1948)

Pall, G., [1] On sums of squares, *Amer. Math. Monthly* **40** (1933) 10–18.

Patz, W., [1] *Tafel der regelmässigen Kettenbrüche und ihrer vollständigen Quotienten für die Quadratwurzeln aus den natürlichen Zahlen von* 1–10000 (Berlin 1955)

Pawlak, Z. and Wakulicz, A., [1] Use of expansions with a negative basis in the arithmometer of a digital computer, *Bull. Acad. Polon. Sci., Cl.* III, **5** (1957) 233–236.

Peano, G., [1] *Formulaire de Mathématique* (Torino 1901)

Pépin, T., [1] Sur certains nombres complexes de la forme $a+b\sqrt{-c}$, *J. Math. Pures Appl.* (3) **1** (1875) 317–372.

Perron, O., [1] *Die Lehre von den Kettenbrüchen* I (Stuttgart 1954).

Piccard, S., [1] *Sur les ensembles de distances des ensembles de points d'un espace euclidien* (Paris 1939)

Pillai, S.S., [1] On some empirical theorem of Scherk, *J. Indian Math. Soc.* **17** (1927–28) 164–171.

[2] On some functions connected with $\varphi(n)$, *Bull. Amer. Math. Soc.* **35** (1929) 832–836.

[3] On Waring's problem II, *J. Indian Math. Soc.* (*N.S*) **2** (1936) 16–44.

[4] On *m* consecutive integers I, *Proc. Indian Acad. Sci., Sect. A* **12** (1940) 6–12.

[5] On *m* consecutive integers III. *Proc. Indian Acad. Sci., Sect. A* **13** (1941) 530–533.

[6] On *m* consecutive integers IV, *Bull. Calcutta Math. Soc.* 36 (1944) 99–101.

[7] On the smallest primitive root of a prime, *J, Indian Math. Soc.* (*N. S*) **8** (1944) 14–17.

[8] On the equation $2^X-3^Y = 2^x+3^y$, *Bull. Calcutta Math. Soc.* 37 (1945) 15–20.

Pipping, N., [1] Neue Tafeln für das Goldbachsche Gesetz nebst Berichtigungen zu den Haussnerschen Tafeln, *Comment. Phys. Math.* 4 (1027–29) no 4.

[2] Über Goldbachsche Spaltungen grosser Zahlen, *Comment. Phys. Math.* 4 (1927–29) no 10.

Pocklington, H.C., [1] Some diophantine impossibilities, *Proc. Cambridge Philos. Soc.* **17** (1914) 108–121.

Podsypanin, V.D., [1] On a property of Pythagorean numbers (in Russian), *Izv. Vyssh. Uchebn. Zaved. Matematika* 1962, no 4 (29) 130–133.

van der Pol, B., and Speziali, P., [1] The primes in $k(\varrho)$, *Indag. Math.* **13** (1951) 9–15.

de Polignac, A., [1] Six propositions arithmologiques déduites du crible d'Eratosthène, *Nouv. Ann. Math.* **8** (1849) 423–429.

Pollock, F., [1] On the extension of the principle of Fermat's theorem of the polygonal numbers to the higher orders of series whose ultimate differences are constant. With a new theorem proposed, applicable to all the orders, *Proc. Roy. Soc. London* **5** (1851) 922–924.

Pollack, R.M., and Shapiro, H.N., [1] The next to the last case of a factorial diophantine equation, *Comm. Pure Appl. Math.* **26** (1973) 313–325.

Polya G. and Szegö G., [1] *Aufgaben und Lehrsätze aus der Analysis*, Bd II (Berlin 1925).

Pomerance, C., [1] On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$, *Acta Arith.* **26** (1975) 265–272.

[2] On the distribution of amicable numbers II, *J. Reine Angew. Math.* **325** (1981) 183–188.

[3] On the distribution of pseudoprimes, *Math. Comp.* 37 (1981) 587–593.

[4] A new lower bound for the pseudoprime counting function, *Illinois J. Math.* **26** (1982) 4–9.

Pomerance, C., Selfridge, J.L. and Wagstaff, S.S. Jr., [1] The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.* **35** (1980) 1003–1026.

Porges, A., [1] A set of eight numbers, *Amer. Math. Monthly* **52** (1945) 379–382.

Postnikov, M.M., [1] *Magicheskie kvadraty* (*Magic Squares*, in Russian) (Moscow 1964).

Poulet, P., [1] *La chasse aux nombres, Fasc.* 1 (Bruxelles 1929)

[2] Table de nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100000000, *Sphinx* **8** (1938) 42–52.

[3] Suites de totalics en départ de $n \leqslant 2000$, Hectographed copy in possession of D.H. Lehmer, cf. *Math. Tables Aids Comp.* 3 (1948) 120.

Prachar, K., [1] *Primzahlverteilung* (Berlin–Göttingen–Heidelberg 1957, reprint 1978).

Pritchard, P.A., [1] Long arithmetic progressions of primes: some old, some new, *Math. Comp.* **45** (1985) 263–267.

Rado, R., [1] Some solved and unsolved problems in the theory of numbers, *Math. Gaz.* **25** (1941) 72–77.

Ramanujan, S., [1] Problem 465, *J. Indian Math. Soc.* **5** (1913) 120.

[2] On the expression of a number in the form $ax^2+by^2+cz^2+du^2$, *Proc. Cambridge Philos. Soc.* **19** (1917) 11–21.

Rankin, R.A., [1] Sets of integers containing no more than a given number of terms in arithmetical progression, *Proc. Royal Soc. Edinburgh Sect. A* **65** (1960/61) 318–331.

Reichardt, H., [1] Über die Diophantische Gleichung $ax^4+bx^2y^2+cy^4 = ez^2$, *Math. Ann.* **117** (1940) 235–276.

Ricci, G., [1] Sull'andamento della differenza di numeri primi consecutivi, *Riv. Mat. Univ. Parma* **5** (1954) 3–54.

[2] Sull'insieme dei valori di condensazione de rapporto $(p_{n+1}-p_n)/\ln p_n$ $(n = 1, 2, 3, \ldots)$, *Riv. Mat. Univ. Parma* **6** (1955) 353–361.

Richert, H.-E., [1] Über Zerlegungen in paarweise verschiedene Zahlen, *Norsk Mat. Tidssk.* **31** (1949) 120–122.

[2] Über Zerfällungen in ungleiche Primzahlen, *Math. Z.* **52** (1950) 342–343.

te Riele, H.J.J., [1] New very large amicable pairs, in: *Number Theory, Noordwijkerhout 1983*, (ed H. Jager) Lecture Notes in Mathematics 1068 (Berlin–Heidelberg–New York–Tokyo 1984).

[2] *Computation of All Amicable Pairs Below* 10^{10}. Report NM-R8503, Centrum voor Wiskunde en Informatica (Amsterdam 1985).

Riesel, H. and Vaughan, R.C., [1] On sums of primes, *Arkiv. Mat.* **21** (1983) 45–74.

Robinson, R.M., [1] Mersenne and Fermat numbers, *Proc. Amer. Math. Soc.* **5** (1954) 842–846.

[2] A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers, *Proc. Amer. Math. Soc.* **9** (1958) 673–681.

de Rocquigny, G., [1] Question 1408, *Intermédiaire Math.* **5** (1898) 268.

Röhr [1] *Zeitschrift Math. Naturw. Unterricht* **50** (1919) 95–96.

Rose, K., and Brudno, S., [1] More about four biquadrates equal one biquadrate, *Math. Comp.* **27** (1973) 491–494.

Rosser, J.B., [1] The n-th prime in greater than $n \log n$, Proc. London Math. Soc. (2) **45** (1939) 21–44.

Rosser, J.B., and Schoenfeld, L., [1] Approximate formulas for some function of prime numbers, *Illinois J. Math.* **6** (1962) 64–89.

[2] Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, *Math. Comp.* **29** (1975) 243–269.

Rota, G.C., [1] The number of partitions of a set, *Amer. Math. Monthly* **71** (1964) 498–504.

Roth, K.F., [1] On certain sets of integers, *J. London Math. Soc.* **28** (1953) 104–109.

Rotkiewicz, A., [1] Sur les nombres composés n qui divisent $a^{n-1} - b^{n-1}$, *Rend. Circ. Mat. Palermo* (2) **8** (1959) 115–116.

[2] Sur les nombres pairs n pour lesquels les nombres $a^n b - ab^n$, respectivement $a^{n-1} - b^{n-1}$, sont divisible par n, *Rend. Circ. Mat. Palermo* (2) **9** (1959) 341–342.

[3] On the properties of the expression $a^n - b^n$ (in Polish), *Prace Mat.* **6** (1961) 1–20.

[4] Démonstration arithmétique d'existence d'une infinité de nombres premiers de la forme $nk+1$, *Enseignement Math.* (2) **7** (1962) 277–280.

[5] Sur les nombres pseudopremiers de la forme $ax+b$, *C.R. Acad. Sci. Paris* **257** (1963) 2601–2604.

[6] On the pseudoprimes of the form $ax+b$, *Proc. Cambridge Philos. Soc.* **63** (1967) 389–392.

[7] Un problème sur les nombres pseudopremiers, *Indag. Math.* **34** (1972) 86–91.

[8] *Pseudoprime Numbers and Their Generalizations* (Novi Sad 1972).

Salem, R. and Spencer, D.C., [1] On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. U.S.A.*, **28** (1942) 561–563.

[2] On sets of integers which do not contain a given number of terms in arithmetical progression, *Nieuw Arch. Wisk.* (2) **23** (1952) 133–143.

Salzer, H., [1] On numbers expressible as the sum of four tetrahedral numbers, *J. London Math. Soc.* **20** (1945) 3–4.

Salzer, H. and Levine, N.J., [1] Tables of integers not exceeding 10000000 that are not expressible as the sum of four tetrahedral numbers, *Math. Tables Aids Comp.* **12** (1958) 141–144.

Sansone, G. and Cassels, J.W.S., [1] Sur le problème de M. Werner Mnich, *Acta Arith.* **7** (1962) 187–190.

Sardi, S. [1] Sulle somme dei divisori dei numeri, *Giorn. Mat. Battaglini* **7** (1869) 112–116.

Sathe, L.G., [1] On a problem of Hardy on the distribution of integers having a given number of prime factors, J. *Indian Math. Soc. N.S.* **17** (1953) 63–141, **18** (1954) 27–81.

Scarowsky, M. and Boyarsky, A., [1] A note on the diophantine equation $x^n + y^n + z^n = 3$, *Math. Comp.* **41** (1984) 235–237.

SCHERK, H.F., [1] Bemerkungen über die Bildung der Primzahlen aus einander, *J. Reine Angew. Math.* **10** (1833) 201–208.

SCHINZEL, A., [1] Sur la décomposition des nombres naturels en somme de nombres triangulaires distincts, *Bull. Acad. Polon. Sci. Cl.* III, **2** (1954) 409–410.

[2] Sur une propriété du nombre de diviseurs, *Publ. Math. Debrecen* **2** (1954) 261–262.

[3] Generalization of a theorem of B.S.K.R. Somayajulu on the Euler's function $\varphi(n)$, *Ganita* **5** (1954) 123–128.

[4] On the equation $x_1 x_2 \dots x_n = t^k$, *Bull. Acad. Polon. Sci. Cl.* III, **3** (1955) 17–19.

[5] Sur un problème concernant la fonction φ, *Czechoslovak Math. J.* **6** (1956) 164–165.

[6] Sur l'équation $\varphi(x) = m$, *Elem. Math.* **11** (1956) 75–78.

[7] Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières, *Enseignement Math.* (2) **4** (1958) 71–72.

[8] Sur l'équation $\varphi(x+k) = \varphi(x)$, *Acta Arith.* **4** (1958) 181–184.

[9] Sur les nombres composés n qui divisent $a^n - a$, *Rend. Circ. Mat. Palermo* (2) **7** (1958) 1–5.

[10] Sur les sommes de trois carrés, *Bull. Acad. Polon, Sci. Sér. Sci. Math. Astr. Phys.* **7** (1959) 307–309.

[11] Sur une conséquence de l'hypothèse de Goldbach, *Bulgar. Akad. Nauk. Izv. Mat. Inst.* 4 (1959) 35–38.

[12] Sur l'équation diophantienne $\sum_{k=1}^{n} A_k x_k^{\vartheta_k} = 0$ (in Polish), *Prace Mat.* 4 (1960) 45–49.

[13] Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers", *Acta Arith.* 7 (1961) 1–8.

[14] On the composite integers of the form $c(ak+b)! \pm 1$, *Nordisk Mat. Tidskr.* **10** (1962) 8–10.

SCHINZEL, A. and SIERPIŃSKI, W., [1] Sur quelques propriétés des fonctions $\varphi(n)$ et $\sigma(n)$, *Bull. Acad. Polon. Sci. Cl.* III, **2** (1954) 463–465.

[2] Sur les sommes de quatre cubes, *Acta Arith.* **4** (1958) 20–30.

[3] Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208, and Corrigendum, *ibidem* **5** (1960) 259.

[4] Sur les congruences $x^x \equiv c \pmod{m}$ et $a^x \equiv b \pmod{p}$, *Collect. Math.* **11** (1959) 153–164.

SCHINZEL, A. and TIJDEMAN, R., [1] On the equation $y^m = P(x)$, *Acta Arith.* **31** (1976) 199–204.

SCHINZEL, A. et WAKULICZ, A., [1] Sur l'équation $\varphi(x+k) = \varphi(x)$, II, *Acta Arith.* **5** (1959) 425–426.

SCHMIDT, W.M., [1] Über die Normalität von Zahlen zu verschiedenen Basen, *Acta Arith.* 7 (1962) 299–309.

SCHNIRELMAN, L., [1] Über additive Eigenschaften von Zahlen, *Math. Ann.* **107** (1933) 649–690.

SCHOENBERG, I.J., [1] Über asymptotische Verteilung reeller Zahlen mod 1, *Math. Z.* **28** (1928) 171–200.

SCHOLOMITI, N.C., [1] An expression for the Euler φ-function, *Amer. Math, Monthly* **61** (1954) 36–37.

SCHOLZ, A. and SCHOENBERG, B., [1] *Einführung in die Zahlentheorie* (Berlin 1955).

Schur, I., [1] Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, *Jber. Deutsch. Math. Verein.* **25** (1916) Abt. 1, 114–117.

[2] Einige Sätze über Primzahlen mit Anwendung auf Irreduzibilitätsfragen, *S.-B. Preuss. Akad. Wiss. Phys. Math. Kl.* **23** (1929) 1–24.

Segal, S.L., [1] On $\pi(x+y) \leqslant \pi(x) + \pi(y)$, *Trans. Amer. Math. Soc.* **104** (1962) 523–527.

Segre, B., [1] A note on arithmetical properties of cubic surfaces, *J. London Math. Soc.* **18** (1943) 24–31.

Selberg, A., [1] An elementary proof of the prime-number theorem, *Ann. of Math.* (2) **50** (1949) 305–313.

[2] Note on a paper by L.G. Sathe, *J. Indian Math. Soc.*, (*N.S.*) **18** (1953) 83–87.

Selmer, E.S., [1] The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* **85** (1951) 203–362.

[2] The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. Completion of the tables, *Acta Math.* **92** (1954) 191–197.

[3] The rational solutions of the Diophantine equation $\eta^2 = \xi^3 - D$ for $|D| \leqslant 100$, *Math. Scand.* **4** (1956) 281–286.

Selmer, E.S. and Nesheim, G., [1] Tafel der Zwillingsprimzahlen bis 200000, *Norske Vid. Selsk. Forh.* (Trondheim) **15** (1942) 95–98.

Sexton, C.R., [1] Counts of twin primes less than 100000, *Math. Tables Aids Comp.* **8** (1954) 47–49.

[2] Computo del numero delle coppie di numeri primi gemelli comprese fra 100000 et 1100000, distinte secondo ciffre terminali, *Boll. Un. Mat. Ital.* (3) **10** (1955) 99–101.

[3] Abzählung der Vierlingen von 1000000 bis 2000000, *Anz. Österr. Akad. Wiss. Math.-Nat. Kl.* **92** (1955) 236–239.

Shanks, D. [1] A note on Gaussian twin primes, *Math. Comp.* **14** (1960) 201–203.

Shanks, D. and Wrench, W.J., Jr., [1] Calculation of π to 100000 decimals, *Math. Comp.* **16** (1962) 76–99.

[2] Calculation of e to 100000 decimals, deposited in the UMT file, cf. *Math. Comp.* **23** (1969) 679.

Shorey, T.N., and Tijdeman, R. [1] New applications of Diophantine approximations to Diophantine equations, *Math. Scand.* **39** (1967) 5–18.

Sierpiński, W., [1] Sur un problème du calcul des fonctions asymptotiques (in Polish), *Prace Mat. Fiz.* 17 (1906) 77–118.

[2] Sur les rapports entre les propriétés fondamentales du symbole de Legendre (in Polish), *C.R. Soc. Sci. Lettr. Varsovie* **2** (1909) 260–273.

[3] Sur quelques algorithmes pour développer les nombres réels en séries (in Polish), *C.R. Soc. Sci. Lettr. Varsovie* **4** (1911) 56–77.

[4] Sur un algorithme pour développer les nombres réels en séries rapidement convergentes, *Bull. Acad. Sci. Cracovie, Cl. Sci. Math. Série A*, 1911, 113–117.

[5] Démonstration élementaire d'un théorème de M. Borel sur les nombres absolument normaux et détermination effective d'un tel nombre, *Bull. Soc. Math. France* **45** (1917) 125–132.

[6] Remarque sur une hypothèse des Chinois concernant les nombres $(2^n - 2)/n$, *Colloq. Math.* **1** (1947) 9.

[7] *Działania nieskończone* (*Infinite Operations*, in Polish) (Warszawa–Wrocław 1948).

[8] Remarques sur la décomposition des nombres en sommes des carrés de nombres impairs, *Colloq. Math.* **2** (1949) 52–53.

[9] Contribution à l'étude des restes cubiques, *Ann. Soc. Polon. Math.* **22** (1949) 269-272.

[10] Un théorème sur les nombres premiers, *Mathematiche* (*Catania*) **5** (1950) 66-67.

[11] Sur les puissances du nombre 2, *Ann. Soc. Polon. Math.* **23** (1950) 246-251.

[12] *Teoria liczb* (*Theory of Numbers*, in Polish) Warszawa-Wrocław 1950.

[13] Une proposition de la géométrie élémentaire équivalente à l'hypothèse du continu, *C.R. Acad. Sci. Paris* **252** (1951) 1046-1047.

[14] Sur une propriété des nombres premiers, *Bull. Soc. Roy. Sci. Liège* **21** (1952) 537-539.

[15] Remarques sur les racines d'une congruence, *Ann. Polon. Math.* 1 (1954) 89-90.

[16] Sur une propriété des nombres naturels, *Ann. Mat. Pura Appl.* (4) **39** (1955) 69-74.

[17] On the equation $3^x+4^y = 5^z$ (in Polish), *Wiadom. Mat.* (2) **1** (1955/56) 194-195.

[18] Sur une propriété de la fonction $\varphi(n)$, *Publ. Math. Debrecen* **4** (1956) 184-185.

[19] Sur quelques problèmes concernant les points aux coordonnées entières, *Einseignement Math.* (2) **4** (1958) 25-31.

[20] Sur les nombres premiers de la forme n^n+1, *Enseignement Math.* (2) **4** (1958) 211-212.

[21] Sur les ensembles de points aux distances rationelles situés sur le cercle, *Elem. Math.* **14** (1959) 25-27.

[22] *Cardinal and Ordinal Numbers* (Warszawa 1959).

[23] Sur l'équivalence de deux hypothèses concernant les nombres premiers, *Bulgar, Akad. Nauk. Izv. Mat. Inst.* **4** (1959) 3-6.

[24] Sur les sommes égales des cubes distincts de nombres naturels, *Bulgar. Akad. Nauk. Izv. Mat. Inst.* **4** (1959) 7-9.

[25] Sur les nombres premiers ayant des chiffres initiaux et finals donnés. *Acta Arith.* **5** (1959) 265-266.

[26] *Teoria liczb, Część II* (*Theory of Numbers, Part II*, in Polish) (Warszawa 1959).

[27] Sur les nombres dont la somme des diviseurs est une puissance du nombre 2. *The Golden Jubilee Commemoration Volume* (1958-59) Part I, 7-9 (Calcutta 1963).

[28] Sur un problème concernant les nombres $k \cdot 2^n+1$, *Elem. Math.* **15** (1960) 73-74, and Corrigendum, *ibidem* **17** (1962) 85.

[29] Sur les nombres impairs admettant une seule décomposition en une somme de deux carrés de nombres naturels premiers entre eux, *Elem. Math.* **16** (1961) 27-30.

[30] Sur les nombres triangulaires carrés, *Bull. Soc. Roy. Sci. Liège* **30** (1961) 189-194, and *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* **65** (1961) 1-4.

[31] Démonstration élémentaire d'un théorème sur les sommes de trois nombres premiers distincts, *Glasnik Mat.-Fiz. Astronom. Društvo Mat. Fiz. Hrvatske* (2) **16** (1961) 87-88.

[32] Sur une propriété des nombres triangulaires, *Elem. Math.* **17** (1962) 28.

[33] Sur une propriété des nombres tétraédraux, *Elem. Math.* **17** (1962) 29-30.

[34] Sur quelques conséquences d'une hypothèse de M.A. Schinzel, *Bull. Soc. Roy. Sci. Liège* **31** (1962) 317-320.

[35] *Pythagorean triangles* (New York 1962).

[36] Sur une propriété des nombres naturels, *Elem. Math.* **19** (1964) 27-29.

SISPANOV, S., [1] On pseudo-prime numbers (in Spanish), *Bol. Mat.* **14** (1941) 99-106.

SKOLEM, T., [1] Unlösbarkeit von Gleichungen deren entsprechende Kongruenz für jeden Modul lösbar ist, *Avh. Norske Vid. Akad. Oslo* I, no **4** (1942).

[2] *Diophantische Gleichungen* (Berlin 1938, reprint New York 1950)

[3] On certain distributions of integers in pairs with given differences, *Math. Scand.* **5** (1957) 57–68.

Srinivasan, A.K., [1] Practical numbers, *Current Sci.* **17** (1948) 179–180.

Stark, H.M., [1] A complete determination of the complex quadratic fields of class-number one, *Michigan Math. J.* **14** (1967) 1–27.

[2] Effective estimates of solutions of some diophantine equations, *Acta Arith.* **24** (1973) 251–259.

Steiger, F., [1] Über die Grundlösung der Gleichung $a^2+b^2+c^2 = d^2$, *Elem. Math.* **11** (1956) 105–108.

Stein, M.L. and Stein, P.R. [1] New experimental results on the Goldbach conjecture, *Math. Mag.* **38** (1965) 72–80.

Steinhaus, H., [1] Problem 498 (in Polish), *Matematyka* **10** (1957) No 2, 58.

Steinig, J., [1] On Euler's idoneal numbers, *Elem. Math.* **21** (1966) 73–88.

Stemmler, R.M., [1] The ideal Waring theorem for exponents 401–200000, *Math. Comp.* **18** (1964) 144–146.

Stéphanos, G., [1] Sur une propriété remarquable des nombres incommesurables, *Bull. Soc. Math. France* **7** (1879) 81–83.

Stern, M.A., [1] Über eine der Theilung von Zahlen ähnliche Untersuchung und deren Anwendung auf die Theorie der quadratischen Reste, *J. Reine Angew. Math.* **61** (1863) 66–94.

Steuerwald, R., [1] Ein Satz über natürliche Zahlen mit $\sigma(N) = 3N$, *Arch. Math.* **5** (1954) 449–451.

Stewart, B.M., [1] Sums of functions of digits, *Canadian J. Math.* **12** (1960) 374–389.

[2] Sums of distinct divisors, *Amer. J. Math.* **76** (1954) 779–785.

Storchi, E., [1] Alcuni criteri di divisibilità per i numeri di Mersenne e il carattere 6^{to}, 12^{mo}, 24^{mo}, 48^{mo} dell'intero 2, *Boll. Un. Mat. Ital.* (3) **10** (1955) 363–375.

Strauss, E., [1] Eine Verallgemeinerung der dekadischen Schreibeweise nebst funktionentheoretischer Anwendung, *Acta Math.* **11** (1887) 13–18.

Subba Rao, K., [1] An interesting property of numbers, *Math. Student* **27** (1959) 57–58.

Swift, E., [1] Solution of the problem 213, *Amer. Math. Monthly* **22** (1915) 70–71.

Sylvester, J.J., [1] On arithmetical series, *Messenger Math.* **21** (1892) 1–19, 87–120.

Szele, T., [1] Une généralisation de la congruence de Fermat, *Mat. Tidsskr. B*, 1948, 57–59.

Szemerédi, E., [1] On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975) 199–245.

Takada, J., [1] Computation of cyclic parts of Steinhaus problem for power 8, *Math. Seminar Notes Kobe Univ.* **7** (1959) 543–546.

Tamura, Y. and Kanada, Y., [1] Calculation of π to 4196239 decimals based on Gauss–Legendre algorithm (preprint), cf. *Canadian Math. Bull.* **27** (1984) 443.

Tardy, P., [1] Transformazione di un prodotto di n fattori, *Ann. Sc. Mat. Fis.* **2** (1851) 287–291.

Tchacaloff, L. et Karanicoloff, C., [1] Résolution de l'équation $Ax^m+By^n = z^p$ en nombres rationnels, *C.R. Acad. Sci. Paris* **210** (1940) 281–283.

Teilhet, P.F., [1] Equations indéterminées, *Intermédiaire Math.* **12** (1905) 209–210.

Teuffel, R., [1] Beweise für zwei Satze von H.F. Scherk über Primzahlen, *Jber. Deutsch. Math. Verein.* **58** (1955) Abt. 1, 43–44.

THUE, A., [1] Suggestions to a method in number theory (in Norwegian), *Vid. Selsk. Forhandlinger Kristiania* 1902 No 7.

[2] Über die Unlösbarkeit der Gleichung $ax^2+bx+c = dy^n$ in grossen ganzen Zahlen x und y, *Arch. Math. Naturvid.* **34** (1917) No 16.

TIETZE, H., [1] Tafel der Primzahl-Zwillinge unter 300000, *S.-B. Bayer. Akad. Wiss. Math. Nat. Kl.* 1947, 57–62.

TIJDEMAN, R., [1] On the equation of Catalan, *Acta Arith.* **29** (1976) 197–207.

TROST, E., [1] Aufgabe 79, *Elem. Math.* **6** (1951) 18–19.

[2] Bemerkung zu einem Satz über Mengen von Punkten mit ganzzahligen Entfernungen, *Elem. Math.* **6** (1951) 59–60.

[3] *Primzahlen* (Basel-Stuttgart 1953, 2nd ed. 1968).

TUNNEL, J. B., [1] A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.* **72** (1983) 323–334.

TURÁN, P., [1] Results of number theory in the Soviet Union (in Hungarian), *Mat. Lapok* **1** (1950) 243–266.

TURSKI, S., [1] Décomposition de nombres entiers en sommes de carrés de nombres impairs, *Bull. Soc. Roy. Sci. Liège* **2** (1933) 70–71.

UHLER, H.S., [1] Many figure approximations to $\sqrt{2}$ and distribution of digits in $\sqrt{2}$ and $1/\sqrt{2}$, *Proc. Nat. Acad. Sci. U.S.A.* **37** (1951) 63–67.

[2] A brief history of the investigations on Mersenne numbers and the latest immense primes, *Scripta Math.* **18** (1952) 122–131.

[3] On the 16th and 17th perfect numbers, *Scripta Math.* **19** (1953) 128–131.

USPENSKY, J.V. and HEASLET, M.A., [1] *Elementary Number Theory* (New York and London 1939)

VAHLEN, Th., [1] Beiträge zu einer additiven Zahlentheorie, *J. Reine Angew. Math.* **112** (1893) 1–36.

VAUGHAN, R.C., [1] On Waring's problem for smaller exponents, *Proc. London Math. Soc.* (3) **52** (1986) 445–463.

[2] On Waring's problem for sixth powers, *J. London Math. Soc.* (2) 33 (1986) 227–236.

VEHKA, T., [1] Explicit construction of an admissible set for the conjecture that sometimes $\pi(x+y) > \pi(x)+\pi(y)$, *Notices Amer. Math. Soc.* **26** (1979) A-453.

VIJAYARAGHAVAN, T., [1] The general rational solution of some Diophantine equations of the form $\sum_{r=1}^{k+1} A_r X_r^{n_r} = 0$, *Proc. Indian Acad. Sci., Sect. A*, **12** (1940) 284–289.

WAGSTAFF, S. S., Jr., [1] On k-free sequences of integers, *Math. Comp.* **26** (1972) 767–771.

[2] Greatest of the least primes in arithmetic progressions having a given modulus, *Math. Comp.* 33 (1979) 1073–1080.

WAKULICZ, A., [1] On the equation $x^3+y^3 = 2z^3$, *Colloq. Math.* **5** (1957) 11–15.

WALKER, G.W., [1] Solution of the problem E 985, *Amer. Math. Monthly* **59** (1952) 253.

WALSH, C.M., [1] Fermat's Note XIV, *Ann. of Math.* (2) **29** (1928) 412–432.

WARD, M., [1] A type of multiplicative diophantine systems, *Amer. J. Math.* **55** (1933) 67–76.

WATSON, G.L., [1] A proof of the seven-cube theorem, *J. London Math. Soc.* **26** (1951) 153–156.

[2] Sums of eight values of a cubic polynomial, *J. London Math. Soc.* **27** (1952) 217–224.

WATSON, G.N., [1] The problem of the square pyramid, *Messenger Math.* **48** (1918) 1–22.

WEINBERGER, P., [1] Exponents of the class groups of complex quadratic fields, *Acta Arith.* **22** (1972) 117–124.

WEINTRAUB, S., [1] A large prime gap, *Math. Comp.* **36** (1981) 279.

WERTHEIM, G., [1] *Anfangsgründe der Zahlenlehre* (Braunschweig 1902)

WHITEHEAD, E.G., [1] The Ramsey number $N(3,3,3,3;2)$, *Discrete Mathematics* **4** (1973) 389–396.

WHITTEN, S., [1] Tables of the totient and reduced totient function, Manuscript deposited in UMT file, cf. *Math. Tables Aids Comp.* **4** (1950) 29–31.

WHITWORTH, W.A., [1] *Choice and Chance with One Thousand Exercises* (Cambridge 1901, reprint New York 1951).

van WIJNGARDEN, A., [1] A table of partitions into two squares with an application to rational triangles. *Indag. Math.* **12** (1950) 313–325.

WILLEY, M., [1] Solution of the problem E 68, *Amer. Math. Monthly* **41** (1934) 330.

WILLIAMS, H.C. and DUBNER, H., [1] The primality of R 1031, *Math. Comp.* **47** (1986) 703–711.

WIRSING, E., [1] Bemerkung zu der Arbeit über vollkommene Zahlen, *Math. Ann.* **137** (1959) 316–318.

WÓJCIK, J., [1] On sums of three squares, *Colloq. Math.* **24** (1971) 117–119.

WUNDERLICH, M., [1] Certain properties of pyramidal and figurate numbers, *Math. Comp.* **16** (1962) 482–486.

[2] On the Gaussian primes on the line Im $(X) = 1$, *Math. Comp.* **27** (1973) 399–400.

YANNEY, B.F., [1] Another definition of amicable numbers and some of their relations to Dickson's amicables, *Amer. Math. Monthly* **30** (1923) 311–315.

YATES, S., [1] Sinkers of titanics, *J. Recreational Math.* **17** (1984/85) 268–274.

YORINAGA, M., [1] Numerical investigation of some equations involving Euler's φ-function, *Math. J. Okayama Univ.* **20** (1978) 51–58.

ZAHLEN, J.P., [1] Sur les nombres premiers à une suite d'entiers consécutifs, *Euclides* (Madrid) **8** (1948) 115–121.

ZAJTA, A.J., [1] Solutions of the Diophantine equation $x^4+y^4 = z^4+t^4$, *Math. Comp.* **41** (1983) 635–659.

ZARANKIEWICZ, K., [1] On triangular numbers (in Polish), *Matematyka* **2** (1949), No 4, 1–7 and No 5, 1–8.

Added in proof

BEDOCCHI, E., [1] Nota ad una congettura sui numeri primi, *Riv. Mat. Univ. Parma* (4) **11** (1985) 229–236.

AUTHOR INDEX

Abbot, H. L., 440
Aigner, A., 374
Alaoglu, L., 177, 181
Ankeny, N. C., 391
Anning, N. H., 387
Artin, E., 274
Atkin, A. O. L., 121
Avanesov, E. T., 87, 289

Bachmann, P., 348, 438, 474
Baillie, R., 249, 373
Baker, A., 105
Baker, C. L., 119
Balasubramanian, R., 427, 428
Balog, A., 252
Bang, A. S., 427
Bang, T., 367
Baumert, L. D., 440
Beck, W. E., 184
Bedocchi, E., 218
Beeger, N. G. W. H., 231, 373
Behrend, F. A., 442, 443
Bell, E. T., 70
Bendz, T. R., 108
Bernoulli, Johannes, 431
Bertrand, J., 145
Best, M. R., 81
Beyer, W. A., 99
Bieberbach, L., 436, 438
Blanusa, D., 118
Blundon, W. J., 420
Bochner, S., 22
Bohman, J., 121, 122, 136
Borel, E., 99, 299
Borho, W., 187
Borozdkin, K. G., 124
Bouniakowsky, V., 108, 132, 135
Bourger, M., 298
Boyarsky, A., 34
Brauer, A., 8, 31, 104
Bredihin, B. M., 132
Bremner, A., 87
Brent, R. P., 120, 121, 154–156, 371
Briggs, W. E., 229
Brillhart, J., 216, 368, 371
Bromhead, T., 61
Brouwer, L. E. J., 298
Browkin, J., 8, 85, 248, 386, 415, 444
Brown, A. L., 184
Brown, J. L. Jr., 18, 153
Brudno, S., 55
Brun, V., 121, 123
Buck, R. C., 130
Buhler, J. P., 215
Buxton, M., 181

Calloway, A., 393
Calloway, J., 393
Cantor, G., 301, 302
Carmichael, R. D., 69, 233, 252, 253, 256, 266, 415
Cassels, J. W. S., 79, 106, 107, 458
Catalan, E., 177
Cattaneo, P., 184
Cauchy, A., 220
Cel, J., 75
Chakrabarti, M. C., 394
Champernowne, G. D., 300
Chein, E. Z., 86, 109
Chen, J. R., 123, 155, 428
Chernick, J. 232
Chikawa, K., 289
Choi, S. L. G., 202
Chojnacka-Pniewska, M., 204
Chowla, S., 127, 229
Cipolla, M., 230
Clement, P. A., 117, 224
Coblyn, 224

Coghlan, E. B., 105
Cohen, E., 168
Cohen, G. L., 185, 250
Cohen, H., 179
Colombo, M., 120
de Comberousse, C., 50
Copeland, A. H., 300
Cormack, G. V., 373
van der Corput, J. G., 123, 127, 385, 445
Coustal, R., 99
Coxe, C., 132
Cramer, H. 156
Crandall, R. E., 215
Crocker, R., 447, 448
Cunningham, A. J. C., 371, 373

Danilov, L. V., 105
Davenport, H., 202, 220, 429
Dem'yanenko, V. A., 40, 109, 111, 422
Denes, P., 86
Depman, I. Ya., 119
Desboves, A., 123
Descartes, R., 184, 186, 187, 402
Deshouillers, J.-M., 427, 428
Devitt, J. S., 177
Dickson, L. E., 61, 62, 117, 125, 126, 132, 133, 177, 187, 214, 217, 229, 401, 429, 430
Diophantus, 32
Dirichlet, P. G. L., 129, 172, 391, 474
Dixon, J. D., 18
Dress, F., 427, 428, 430
Dressler, R., 153
Dubner, H., 117
Duparc, H. J. A., 231, 233
Dutka, J., 99
Dyer Bennet, J., 276

Elmore, S., 181
Eratosthenes, 118
Erdös, P., 81, 86, 87, 112, 120, 122, 123, 136, 145, 160, 162, 169, 176, 181, 188, 202, 224, 232, 251–254, 300, 387, 388, 427, 442, 443, 445
Estermann, T., 31, 268
Euclid, 184
Euler, L., 55, 62, 85, 104, 117, 187, 194, 216, 229, 245, 371, 431, 468

Faber, G., 301
Fauquembergue, E., 368
Fermat, P., 104, 184, 187, 392
Finkelstein, R., 105
Finsler, P., 158
Forrest, J., 123
Frangui, B., 184
Fredericksen, H., 440
Frenicle de Bessy, B., 436
Frobenius, G., 132
Fröberg, C. E., 214
Früchtl, K., 121
Fueter, R., 106

Gabard, E., 3
Gabowicz, J. A., 423
Gałgowski, J., 120
Garcia, M. 184
Gardiner, V. L., 419
Gasper, R. W., Jr, 311
Gauss, K. F., 202, 220, 245, 348, 391
Gelfond, A. O., 295
Georgiev, G., 109
Gerono, C. G., 361
Gilbreath, N. L., 156
Gillard, P., 249
Gillies, D. B., 368
Gilloud, J., 298
Ginsburg, J., 38
Giuga, G., 218
Glaisher, J. W. L., 169, 297
Godwin, H. J., 419
Goldbach, Chr., 86, 123
Golomb, S. W., 121, 360
Golubew, W. A., 121, 132, 134
Goodstein, E., 438
Gostin, G. B., 372
Graham, S., 155
Grosswald, E., 128, 229, 393, 481
Grube, F., 229
Gruenberger, F. J., 119

Gupta, H., 179, 380
Gusev, V. A., 289
Guy, R. K., 177

Hadamard, J., 162
Hadwiger, H., 388
Hagis, P. Jr, 128, 183, 185, 250
Halcke, P., 60
Hall, M. Jr, 105, 328, 444
Hallyburton, J. R., 371
Halter-Koch, F., 407
Hammond, N., 123
Hanly, V. S., 129
Hanson, D., 440
Hardy, G. H., 420
Harris, V. C., 166
Hasse, H., 274, 362
Hausdorff, F., 311
Haussner, R., 154
Heaslet, M. A., 63, 64, 104
Heath-Brown, D. R., 169
Hecke, E., 130
Hemer, O., 104, 105
Hensel, K., 6
Hensley, D., 164
Hilbert, D., 427
Hill, J. D., 63, 64
Hooley, C., 31
Hoffman, H., 187
Hornfeck, B., 184
Hunsucker, J. L., 177
Hurwitz, Adolf, 337, 406
Hurwitz, Alexander, 368, 371
Hyyrö, S., 79

Ibn Al-Banna, 187
Ingham, A. E., 154
Irving, R. W., 441
Iseki, K., 289
Ivic, A., 385
Iwaniec, H., 132

Jacobi, C., 352, 474
Jacobsthal, E., 220
Jaeschke, G., 373
Jakóbczyk, F., 374
Jankowska, S., 253
Jeśmanowicz, L., 40
de Joncourt, E., 84
Jones, B., 392
Jordan, C., 259
Józefiak, T., 40, 84

Kacperek, L., 120
Kalmar, L., 145
Kanada, Y., 298
Kanold, H. J., 177, 188
Kaprekar, D. R., 288
Karanicoloff, C., 109
Keller, W., 372, 373
Khatri, M. N., 84
Khinichin, A. Ya., 427
Killgrove, R. B., 156
Klee, V. L. Jr, 249, 253, 259
Knödel, W., 233
Ko Chao, 40, 111
Kogbetlianz, E., 380
Kolesnik, G., 173
Korec, I., 61
Korhonen, O., 108
Kraitchik, M., 61, 117, 324, 326–328, 363, 372
Krikorian, A., 380
Krishnawami, A. A., 49
Kulik, J. Ph., 119
Kulikowski, T., 224, 386
Kusakabe, T., 289

Lagarias, J. C., 136
Lagrange, Jean, 62
Lagrange, J. L., 328, 427
Lal, M., 249, 420
Lamé, G., 17
Landau, E., 121, 163, 379, 391, 394
Lander, L. J., 55, 120, 122, 154–156, 427
Landry, F., 371
Langevin, M., 79
Lazarus, R. B., 419
Lebesgue, H., 299

Lebesgue, V. A., 102, 108
Lee, E. J., 187
Leech, J., 61, 218
Legendre, A. M., 59, 155, 184, 220, 334
Lehmer, D. H., 3, 49, 136, 216, 230, 232, 250, 363, 368, 400, 419
Lehmer, D. N., 119
Leibniz, G. F., 229, 431
Lerch, M., 225
Leszczyński, B., 109
LeVeque, W. J., 162, 164, 440
Levine, N. J., 88
Lietzmann, W., 202
Light, W. A., 123
Lind, C. E., 77
Lindenbaum, A., 445
Linnik, Yu. V., 155, 427, 429
Liouville, J., 225
Littlejohn, J. C., 420
Littlewood, J. E., 163, 218
Litver, E. L., 275
Ljunggren, W., 81, 85, 86, 108
Lochs, G., 310
London, H., 104
Lucas, E., 81, 302, 368, 371, 429
Lu Wen-Twan, 40

Maciąg, S., 234
Madachy, J. S., 187
Mac Mahon, P., 431
Mahler, K., 429
Maknis, M., 130
von Mangoldt, H., 194
Margenstern, M., 181
Masai, P., 252
Masłowski, S., 444
Mason, Th. E., 187
Mayah, B. H., 125
Mazur, S., 181
Mąkowski, A., 79, 153, 177, 185, 187, 234, 249, 270, 350, 423, 436, 437, 442, 443
McCurley, K. S., 429
Melnikov, J. G., 229
Mersenne, M., 184, 186
Metropolis, N., 99
Meyl, A., 87
Mientka, W. E., 177
Miller, V. S., 136
Mirsky, L., 169
Moessner, A., 437, 438
Mordell, L. J., 31, 34, 101, 103, 104, 391, 419, 422
Morehead, J. C., 371, 377
Moret-Blanc, 110
Morrison, M. J., 371
Morrow, D. C., 234
Moser, L., 81, 216, 249, 442
Muir, T., 320
Müller, M., 288
Mycielski, Jan, 169

Nagell, T., 31, 40, 82, 83, 104, 108, 207, 362
Najar, R. M., 184
Nebb, J., 177
Nesheim, G., 121
Neugerard, J. R., 99
Nickel, E., 368
Niewiadomski, R., 420
Noll, C., 368
Norrie, R., 55

Obláth, R., 111, 298
Odlyzko, A. M., 136
O'Keefe, E. S., 434
Ore, O., 265

Pall, G., 392, 402, 407, 409
Parker, T., 153
Parkin, T. R., 55, 120, 122, 154–156, 427
Patterson, J. O., 55
Patz, W., 327
Pawlak, Z., 290
Paxson, G. A., 371
Peano, G., 297
Pell, J., 99
Penk, M. A., 215
Pepin, T., 104
Perron, O., 320, 323
Pervouchine, I. N., 371, 372
Piccard, S., 445

Pillai, S. S., 7, 8, 80, 149, 251, 274, 429
Pipping, N., 123
Pisano, L. (Fibonacci), 64
Pocklington, H. C., 75
Podsypanin, V. D., 40
van der Pol, B., 132
Poletti, L., 119
de Polignac, A., 445
Pollack, R. M., 112
Pollock, F., 396
Pólya, G., 262
Pomerance, C., 185, 188, 230, 233, 251
Porges, A., 289
Porter, R. J., 119
Postnikov, M. M., 438
Poulet, P., 178, 184, 230, 231
Prachar, K., 163
Pritchard, P. A., 126
Pythagoras, 187

Rado, R., 441
Ralston, K. E., 156
Ramanujan, S., 362, 401
Rankin, R. A., 443
Reichardt, H., 77
Rényi, A., 120
Reynolds, R. L., 31
Ricci, G., 123
Richards, I., 164
Richert, H. E., 152
Rickert, N. W., 121
te Riele, H. J. J., 81, 187
Riesel, H., 124, 368, 372
Robinson, R. M., 368, 373
de Rocquigny, G., 135
Roe, S., 123
Rose, K., 55
Rosser, J. B., 154, 163
Rota, G. C., 432
Roth, K. F., 442, 443
Rotkiewicz, A., 100, 231, 232, 268
Röhr, 87
Russel, W., 420

Salem, R., 442
Salzer, H. E., 87, 88
Sansone, G., 458
Sardi, C., 210
Sathe, L. G., 164
Scarowsky, M., 34
Scherk, H. F., 149
Schinzel, A., 70, 86, 109, 124, 133-135, 153, 155, 156, 169, 177, 215, 226, 232, 249-255, 274, 361, 386, 392, 393, 407, 423
Schmidt, W. M., 300
Schnirelman, L., 124, 427
Schoenberg, B., 30
Schoenberg, I. J., 254
Schoenfeld, L., 154, 163, 164
Scholomiti, N. C., 252
Scholz, A., 30
Schur, I., 145, 440, 443,
Segal, S. L., 164
Segre, B., 420
Selberg, A., 162, 164
Selfridge, J. L., 55, 86, 164, 230, 368, 371, 372
Selmer, E. S., 83, 106, 121
Serret, J. A., 217, 220
Sexton, C. R., 121
Shanks, D., 177, 298, 462
Shapiro, H. N., 112
Shibamura, K., 289
Shorey, T. N., 298
Sierpiński, W., 31, 35, 40, 85, 87, 124, 125, 129, 133-135, 149, 153, 155, 165, 176, 181, 205, 226, 228, 230, 233, 236, 249, 250, 253-255, 266, 274, 275, 279, 299, 301, 303, 327, 336, 341, 361, 362, 374, 375, 385-388, 396, 423, 424, 442, 447
Sispanov, S., 233
Skałba, M., 73
Skolem, T., 99, 207, 434
Skula, L., 154
Slowiński, D., 368
Spencer, D. C., 442
Speziali, P., 132
Srinivasan, A. K., 181
Stark, H. M., 105, 132
Stearns, R. E., 177
Steiger, F., 407
Stein, M. L., 123
Stein, P. R., 123, 419

Steinhaus, H., 385, 386
Steinig, J., 229
Stemmler, R. M., 429
Stephanos, C., 301
Stephens, N. M., 105
Stern, M. A., 432
Steuerwald, R., 184
Stewart, B. M., 181, 289
Stifel, M., 438
Storchi, E., 362
Strauss, E., 301
Subba Rao, K., 288
Swift, D., 202
Swift, E., 56
Sylvester, J. J., 145
Szegö, G., 262
Szekeres, G., 442
Szele, T., 217, 261
Szemerdi, E., 443

Takada, J., 289
Tamura, Y., 298
Tardy, P., 430
Tchacaloff, L., 109
Tchebycheff, P. L., 145
Tebay, S., 61
Teilhet, P. F., 85
Teuffel, R., 149
Thue, A., 30, 104
Tietze, H., 121
Tijdeman, R., 79, 86, 298
Tonascia, J., 216
Trost, E., 81, 129, 131, 136, 158, 162, 165, 363, 388
Tuckerman, B., 368
Tunnell, J. B., 65
Turan, P., 122, 274, 442, 443
Turski, S., 396

Uhler, H. S., 99, 368
Uspensky, J. V., 63, 64, 104

Vahlen, Th., 431
Valette, A., 252
de la Vallée Poussin, Ch., 162
Vaughan, R. C., 124, 429
Vehka, T., 164
Vijayaraghavan, T., 109
Vinogradov, I., 124
Vogt, R. L., 177
Voronoi, G., 173

Wagstaff, S. S. Jr, 155, 230, 368, 442
Wakulicz, Andrzej, 249, 290
Wakulicz, Antoni, 78, 96
Walker, G. W., 442
Walsh, C. M., 56
Ward, M., 70
Waring, E., 427
Watson, G. L., 88, 429
Watson, G. N., 81
Weinberger, P., 216, 229
Weintraub, S., 120
Wertheim, G., 274
Western, A. E., 371
Wheeler, D. J., 368
Whitehead, E. G., 440
Whitten, S., 265
Whitworth, W. A., 432
Wieferich, A., 427, 428
van Wijngarden, A., 379
Willey, M., 41
Williams, H. C., 117, 371, 373
Wirsing, E., 184
Wójcik, J., 391
Woodall, H. J., 373
Wrathall, C. P., 372
Wrench, W. J. Jr, 298
Wright, E. M., 420
Wunderlich, M., 87,132

Yanney, B. F., 187
Yates, S., 121
Yorinaga, M., 249
Yudina, G. E., 275

Zahlen, J. P., 148
Zajta, A. J., 55
Zarankiewicz, K., 53, 84, 254
Zeitlin, D., 129

SUBJECT INDEX

Absolutely normal numbers 299
Absolutely pseudoprime numbers 232
Algorithm
— Euclidean 16, 453
— of continued fractions 16
Almost magic square 438
Amicable numbers 186
Artin's conjecture 274
Associated integers 452

Base of the index 280
Bertrand's postulate 145
Bouniakowsky's conjecture 132
Brouncker's formula 336, 469

Carmichael's conjecture 252
— number 233
Catalan conjecture 79
Catalan-Dickson conjecture 177
Chinese remainder theorem 27
Common divisor 5
— multiple 4
Complex (Gaussian) integers 449
— — prime 459
— — — relatively prime 457
Composite numbers 62
Congruence 198
Congruent numbers 62
Conjecture C 422
— H 133
— P 153
— P_1 155
Continued fractions 19, 304, 335
— — , simple 19, 307
Convergent of a continued fraction 304
Crocker's theorem 447
Cullen numbers 373

Decimal 285
Digit 285
Diophantine equations 32
Dirichlet multiplication 174
D numbers 234
Divisibility 1, 451
Division algorithm 16
Divisor 1, 451
— , common 5
— , greatest common 5, 454

Eisenstein's rule 359
Equation
—, Diophantine 32
—, Pythagorean 35
Eratosthenes sieve 17
Erdös's theorem 445
Euclidean algorithm 16, 453
Euler's conjecture 425
— constant 173
— formulae 468, 469, 481
— identity 399
— numbers 229
— theorems 261, 271
— totient function 245
— trinomial 130

Factorization 115
Fermat equation 88
— Last Theorem 53, 108, 415
— numbers 369
— Simple Theorem 216
— (other) theorems 47, 51, 56, 57, 75, 219, 267, 392
Fibonacci sequence 17
Function $d(n)$ 166
— $\lambda(n)$ (Liouville's) 196
— $\lambda(n)$ (minimum universal exponent) 265

— $\gamma(n)$ 192
— $\pi(n)$ 136
— $\sigma(n)$ 174
— $\varphi(n)$ 245
Fundamental theorem of arthmetic 9

Gaussian integers 449
Gauss's function 245
— lemma 342
— theorem 391
Gilbreath's conjecture 156
Goldbach's conjecture 123
Greatest common divisor 5, 454

Hurwitz's theorem 406

Index of an integer 280
Integers 1
—, complex (Gaussian) 449
—, — associated 452

Jacobi's symbol 352
— theormes 401, 467, 474

Lagrange's theorems 235, 328, 397
Lambert series 174
Lamé's theorem 17
Lattice points 383
Law of quadratic reciprocity 348
— of the best approximation 312
Least common multiple 4, 458
Legendre's symbol 340
Leibniz's theorem 214
Lejeune Dirichlet's theorem 129
— — formula 179
Liouville's function 196
— identity 468
Lucas-Lehmer's theorem 363
Lucas's identity 429
— theorem 366

Magic square 434
— —, perfect 436
Mersenne numbers 184
Minimum universal exponent 265
Möbius function 192
Multiple 1
—, common 4
—, least common 4, 458
Multiply perfect numbers 184

Natural numbers 1
Norm 450
Normal numbers 299
Numbers
—, absolutely normal 299
—, absolutely pseudoprime 232
—, amicable 186
—, composite 113
—, congruent 62
—, *D* 234
—, multiply perfect or P_m 184
—, natural 1
—, normal 299
—, perfect 182
—, practical 181
—, prime 113
—, pseudoprime 229
—, quasi-perfect 184
—, relatively prime 6
—, square-free 31
—, superabundant 181
—, super-Poulet 231
—, tetrahedral 87
—, triangular 44
Numeri idonei 228

Pall's theorems 402, 407, 409
Partitio numerorum 431
Pell's equation 88
— series 302
Perfect magic square 436
— numbers 182
P_m numbers 184
Poulet numbers 231
Power residue 276
Practical numbers 181
Prime complex integers 459
— numbers 113

Prime number theorem 162
Primitive roots 264
Pseudoprime numbers 229
Pythagorean equation 35
— triangle 35

Quadratic irrational 328
— non-residue 211
— reciprocity law 348
— residue 211
Quadruplet of primes 121
Quasi-perfect numbers 184

Rédei's theorem 261
Relatively prime complex integers 457
— — numbers 6
Remainder 203
Richert's theorem 152
Roots of the congruence 203
—, primitive 264
Rule for calculating the greatest common divisor of two numbers 16
— for reducing periodic fractions 296
Rules of divisibility 201

Scherk's theorem 148
Schur's theorem 480
Simple continued fractions
— — —, finite 19
— — —, infinite 307
Square
—, almost magic 438
—, magic 434
—, perfect magic 436
Superabundant numbers 231

Tchebycheff's theorem 145
Tetrahedral numbers 87
Thue's theorem 30
Triangular numbers 44
Triplet of primes 271
Twin primes 120
— —, complex 462

Wallis's formula 469
Waring's theorem 427
Wilson primes 214
— theorem 214

ADDENDUM AND CORRIGENDUM INSERTED IN JULY, 1987

1. The greatest of the known pairs of twin primes is no longer the pair $260497545 \cdot 2^{6625} \pm 1$ mentioned on p. 121, but the pair $107570463 \cdot 10^{2250} \pm 1$, see

   DUBNER H. and DUBNER R., The development of a powerful lower-cost computer for number theory applications, J. Recreational Math. **18** (1985/6), 92–96.

2. The best estimate of the error term in the formula for $T(x)$ on p. 173 and for $T(n)$ on p. 385 is at present due to Iwaniec and Mozzocchi, see

   IWANIEC, H. and MOZZOCCHI, C.J., On the divisor and circle problems, preprint.

   They prove that each error term does not exceed $C(\varepsilon)\, X^{7/22+\varepsilon}$, where X equals x or n, respectively, ε is any positive number and $C(\varepsilon)$ a constant depending only on ε.

3. The information given on p. 229 that Chinese mathematicians claimed 25 centuries ago that $n \mid 2^n - 2$ only for n prime, is wrong. It was based on a statement by J.H. Jeans quoted in Dickson [7], vol. 1, p. 91 and that was apparently due to an error in translation. See

   NEEDHAM J., *Science and Civilization in China*, vol. 3: *Mathematics and the Sciences of the Heavens and the Earth*, Cambridge 1959, p. 54, footnote d.

   The reference to Dickson on p. 229, footnote (2) should be [7], vol. 1, p. 91, not p. 64.

4. The paper [3] of V.A. Demyanenko, quoted on p. 111 contains a serious error and his theorem cannot be regarded as proved. However, if $x^x y^y = z^z$ then either every prime factor of x divides y, or every prime factor of y divides x, see

   SCHINZEL A., Sur l'équation diophantienne $x^x y^y = z^z$ (Chinese), Acta Sc. Nat. Univ. Szechuansis **18** (1958), 81–83.